International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences
(NCDATES- 09th & 10th January 2015)

RESEARCH ARTICLE OPEN ACCESS

A Survey of Information Security in HealthCare Sector

M.Jyothirmai, M.Ashwitha
Assistant.Professor, CMR Engineering College Hyderabad, Telengana, India
Assistant.Professor, CMR Engineering College Hyderabad, Telengana, India

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 exchange between patients, providers and payers, all point towards the need for better information security. We critically survey the literature on information security and privacy in healthcare, published in information systems journals as well as many other related disciplines including health informatics, public health, law, medicine, the trade press and industry reports. In this paper, we provide a holistic view of the recent research and suggest new areas of interest to the information systems community.
Keywords: information security; privacy; healthcare; research literature.

Introduction

Healthcare information systems are largely viewed as the single most important factor in improving US healthcare quality and reducing related costs. According to a recent RAND study, the USA could potentially save $81B annually by moving to a universal Electronic Health Record (EHR) system (Hillestad et al., 2013). Not surprisingly, recent government initiatives have pushed for wide-scale adoption of universal EHR by 2014 (Goldschmidt, 2010). Yet, IT spending in healthcare sector trails that of many other industries, typically 3–5% of revenue, far behind industries like financial services where closer to 10% is the norm (Bartels, 2009). Anecdotal evidences from recent years suggest that a lack of adequate security measures has resulted in numerous data breaches, leaving patients exposed to economic threats, mental anguish and possible social stigma (Health Privacy Project, 2009). A recent survey in the USA suggests that 75% of patients are concerned about health websites sharing information without their permission (Raman, 2007). Possibly, this patient perception is fuelled by the fact that medical data disclosures are the second highest reported breach (Hasan and Yurcik, 2006). In response to these increasing threats to health information and privacy, new regulations at both the state and the federal level have been proposed in the USA, e.g., Health Insurance Portability and Accountability Act (HIPAA).[1]

Over the past two decades, information security research has become a well-established area within the information systems discipline. Researchers have adopted several underlying theories from reference disciplines such as psychology and sociology to analyse information security risk management (Baker et al., 2007; Dhillon and Backhouse, 2001; Straub and Collins, 1990; Straub and Welke, 1998; Vaast, 2007) and economic theories to characterise investment decisions and information governance (Cavusoglu et al., 2004, 2005; Gordon and Loeb, 2002; Khansa and Liginlal, 2009; Kumar et al., 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 the healthcare sector,[2,3] which is heavily regulated and calls upon business models different from other industries.

In this paper, we review the current state of information security and privacy research in healthcare, covering various research methodologies such as design research, qualitative research and quantitative research. Our review illuminates the multifaceted research streams, each focusing on special dimensions of information security and privacy. For example, on the one hand, a large body of research focuses on developing technological solutions for ensuring privacy of patients while their information is stored, processed and shared. On the other hand, several researchers have examined the impact of health IT adoption on care quality. Additionally, the enactment of the HIPAA and emergence of web-based healthcare applications have turned researchers' attention towards patient as well provider perspectives on HIPAA. Surprisingly, very limited attention has been given to the economics of information security risks (e.g., financial risks arising from medical identity theft and healthcare fraud).

In this paper, first we present a general view of information flow in healthcare and the evolving regulatory landscape. Next, we identify several research domains that we use to classify the literature. Building on this classification, we summarize the literature focusing on key application

areas of information security in healthcare. Finally, we conclude by identifying future research directions.

Background of health information privacy and security

Privacy is viewed as a key governing principle of the patient–physician relationship. Patients are required to share information with their physicians to facilitate correct diagnosis and treatment, and to avoid adverse drug interactions. However, patients may refuse to divulge important information in cases of health problems such as psychiatric behaviour and HIV, as their disclosure may lead to social stigma and discrimination (Applebaum, 2002). Over time, a patient's medical record accumulates significant personal information including identification, history of medical diagnosis, digital renderings of medical images, treatments, medication history, dietary habits, sexual preference, genetic information, psychological profiles, employment history, income and physicians' subjective assessments of personality and mental state[4].

Figure 1 shows a typical information flow in the healthcare sector. Patient health records serve a range of purposes apart from diagnosis and treatment provision. For example, information could be used to improve efficiency within the healthcare system, drive public policy development and administration, and in the conduct of medical research (Hodge, 2003). A patient's medical records are also shared with payer organisations (e.g., private insurance or Medicare/Medicaid) to justify payment of services rendered. Healthcare providers also use records to manage their operations and improve service quality. Furthermore, providers may share health information through Regional Health Information Organisations (RHIOs) to facilitate care services.

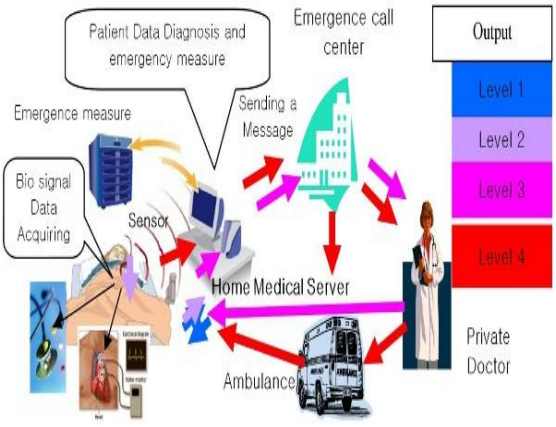

Figure 1 Information flow in the health care system

3State of information security research in healthcare

In this section, we present a comprehensive review of the information security literature in healthcare sector (refer to Appendix 1 for categorisation of papers reviewed in this paper). For this survey, we conducted a multidisciplinary search in a diverse set of publications and fields including information systems, health informatics, public health, medicine and law. Furthermore, we searched for articles in popular trade publications and reports. Figure 2 summarises four primary research domains in the healthcare information security and privacy (depicted as ovals) that intersect with corresponding four domains of information-systems-related research in healthcare (depicted as dotted boxes).

First, research on issues related to healthcare consumers, including personal health record management and web-based EHR systems, have raised a number of security-related topics including the drivers of privacy and security concerns among consumers, monetary impact of privacy and security breaches to consumers, and impact of medical identity theft on consumers' well-being. Second,[5] research focused on issues related to providers, such as the drivers of IT adoption, impact of IT on medical errors, telemedicine, pervasive computing and RFID adoption, also interacts with emerging security issues, for example, the design and development of access control systems, sustainability of information integrity, network security, privacy policy management and risk management. Similarly, research focusing on inter-organisational issues such as health services subcontracting, design and development of inter-organisational health networks, and EDI adoption gives rise to security and privacy research problems such as inter-organisational access control, data interoperability, multi-institutional network security and fraud control. Lastly, several information security and privacy research directions (e.g., development of data interoperability standards, regulatory implications of healthcare technology adoption and secured data disclosure mechanisms) have emerged in the public policy domain, particularly in areas such as medical research, development of national health information network, disaster response and pricing of health services.

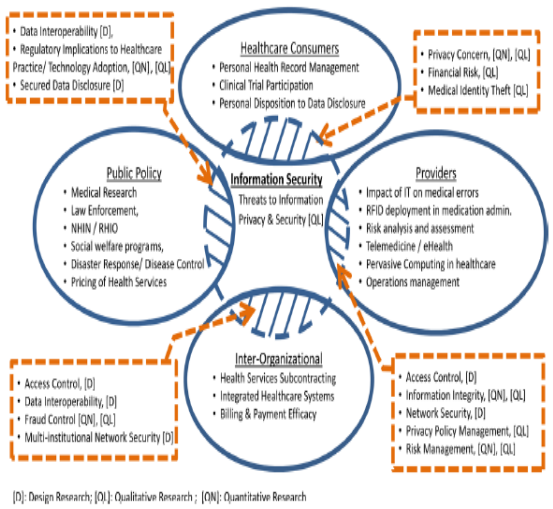

Figure 2 Research domains in the healthcare information security

It is noteworthy that past research has used a diverse range of methodologies, including design research, qualitative research and quantitative research. Design research focuses on developing artefacts such as models, algorithms, prototypes and frameworks to solve specific information system problems (Hevner et al., 2004). In healthcare information security research, we find papers focusing on technological solutions for maintaining patients privacy in a wired and wireless network of a provider organisation, for (authorised) disclosure of patient data for secondary usage such as academic research, and for data sharing in a network of providers (e.g., Dong and Dulay, 2006; Malin, 2007; Malin and Airoldi, 2007). Qualitative research involves examining a social phenomenon using a range of qualitative instruments/data such as interviews, documents, participants' observation data, researcher's observation and impression (Myers, 1997). In healthcare research, much of the qualitative research centres around the impact of HIPAA on healthcare practices (e.g., Ferreira et al., 2006; Hu et al., 2006; Terry and Francis, 2007). Lastly, researchers in healthcare information systems have adopted several quantitative methods including surveys, econometric analysis and statistical modelling in the areas of patients' privacy concern, public policy, fraud control, risk management and impact of health IT on medical errors (Bansal et al., 2007; Koppel et al., 2005; Miller and Tucker, 2009; Rosenberg, 2001a, 2001b).

In the following sections, we present a summary of extant research in each of the research themes identified within the four domains in Figure 2. Research themes, such as access control, that span multiple domains are presented together.

3.1 Threats to information privacy

Although health information privacy has been widely discussed in the social science and business press (Etzioni, 1999), the academic literature lacks systematic investigation to identify and classify various sources of threats to information privacy and security. Recent policy-based studies (such as NRC, 1997; Rindfleisch, 1997) broadly categorise privacy threats, or source of information security, into two areas:

1 organisational threats that arise from inappropriate access of patient data by either internal agents abusing their privileges or external agents exploiting a vulnerability of the information systems
2 systemic threats that arise from an agent in the information flow chain exploiting the disclosed data beyond its intended use (NRC, 1997).

Organisational Threats: These threats assume different forms, such as an employee who accesses data without any legitimate need or an outside attacker (hacker) that infiltrates an organisation's information infrastructure to steal data or render it inoperable. At the outset, these organisational threats could be characterised by four components: motives, resources, accessibility and technical capability (NRC, 1997). Depending on these components, different threats may pose different levels of risk to an organisation requiring different mitigation and prevention strategies. The motives behind these threats could be economic or non-economic. For some (such as insurers, employers and criminals), patient records may have economic value, whereas others may have non-economic motives such as a person involved in a romantic relationship. These attackers may have resources ranging from modest financial backing and computing skills to a well-funded infrastructure. Additionally, the nature of the threats typically depends on the technical capability of the attackers. Moreover, with the growing underground cyber economy (Knapp and Boulton, 2006), an individual possessing adequate financial resources and with the intent to acquire data may be able to buy the services of sophisticated hackers to breach healthcare data. Recent studies suggest that the broad spectrum of organisational threats could be categorised into five levels, listed in increasing order of sophistication (NRC, 1997):

- *Accidental disclosure*: Healthcare personnel unintentionally disclose patient information to others (e.g., e-mail message sent to wrong address or inadvertent web-posting of sensitive data).
- *Insider curiosity*: An insider with data-access privilege pries upon a patient's records out of

curiosity or for their own purpose (e.g., a nurse accessing information about a fellow employee to determine possibility of a sexually transmitted disease or medical personnel accessing potentially embarrassing health information about a celebrity and transmitting it to the media).

- *Data breach by insider*: Insiders access patient information and transmit it to outsiders for profit or revenge.
- *Data breach by outsider with physical intrusion*: An outsider enters the physical facility either by coercion or forced entry and gains access to the system.
- *Unauthorised intrusion of network system*: An outsider, including former employees, patients, or hackers, intrudes into an organisation's network from the outside to gain access to patient information or render the system inoperable.

3.2 Privacy concern among healthcare consumers:

A significant body of research has examined the perception of privacy concerns from the 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 other at-risk family members.

This extensive body of research has primarily focused on the use of identifiable or potentially identifiable information by others outside of immediate health providers, such as employers, families and third parties (Sankar et al., 2003). However, very limited research has examined patients' perceptions of sharing anonymised health records (perhaps with the exception of more recent studies that examine patients' perceptions about consent for data use (Bansal et al., 2007; Campbell et al., 2007)).

Only about 10% of the patients expected to be asked for permission if their doctors used their health information for a wide variety of purposes, including combining data with other patients' data to provide better information to future patients, sharing treatment outcomes with other physicians, teaching medical professionals and writing research articles about diseases and treatments.

3.3 Providers' perspective of regulatory compliance:

Patients' health information, including medication history, is critical to medical research for improving healthcare quality. However, disclosure of health information to researchers raises concerns of privacy violations. Regulations such as HIPAA allow healthcare organisations to disclose otherwise protected health information to researchers only if they have obtained consent from patients or, in exceptional cases, on approval from an Institutional Review Board (IRB). Anecdotal evidence suggests that the new regulatory requirements have had an adverse effect on the conduct of medical research (e.g., Kaiser, 2004, 2006; Turner, 2002). In a survey of epidemiologists, Ness (2007) reports that nearly 68% of researchers felt that HIPAA made medical research 'highly difficult' and only about 25% believed that it has increased patients' confidentiality or privacy. More importantly, about 39% of researchers believed that HIPAA had increased research cost by a 'great deal', especially owing to additional compliance-related administrative cost and about 51% of researchers believed HIPAA enforcement lead to delays in research. In a critical review of three cases of health research projects, Shen et al. (2006) report that the complexity of consent and privacy protection forms are time-consuming and cost-amplifying procedures that often get in the way of patient recruitment. The authors recommend simplifying the language of privacy and consent forms to facilitate comprehension by patients. Furthermore, if a breach of confidentiality is the primary risk and the quality of the project could be affected from reduced participation, the authors suggest discarding the consent process and instead publish a statement on potential use of PHI in a "Notice of Privacy Practices" allowing patients to make informed choices.

3.4 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 organisational boundaries. Role-Based Access Control (RBAC), originally developed to manage access to resources in a large computer network Sandhu et al., is generally presented as an effective tool to manage data access 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. This stream of research primarily focuses on developing algorithms and frameworks to facilitate role-based information access.). To improve the transparency of access control management, some hospital systems have even adopted the policy of sharing audit logs with patients, thus enabling them to continually refine access rights on their own health records.

3.5 Data interoperability and information security:

Many healthcare information systems currently in use store information in different proprietary formats. This diversity of data formats creates a major hurdle in sharing patient data among provider organisations, not to mention data for research. Development of a fully functional interoperable EHR system remains a major challenge. Recent research has proposed prototypes of Service-Oriented Architecture (SOA) models for EHR in various contexts including clinical decision support (Catley et al., 2004), collaborative medical (mammogram) image analysis (Estrella et al., 2004) and health clinic settings (Raghupathi and Kesh, 2007). These SOA-based EHRs are expected to be scalable to enable inter-enterprise environments, such as RHIO, and alliances of such RHIOs could lead to national and global health information networks (Raghupathi and Kesh, 2007). Using a case study analysis of three emerging RHIOs (namely the Indian health Information Exchange, the Massachusetts Health Data Consortium and the Santa Barbara County Care Data Exchange), Solomon (2007) elicited several factors that influence innovation and diffusion, adaptation and change management of RHIOs. Among them, privacy and security of patient information are major concerns hampering the adoption of clinical information technologies across the RHIOs and consumers. Such concerns could remain in the near future, as the technology standards for data interoperability are still in the development stage (Dogac et al., 2006; Eichelberg et al., 2005). Moreover, Solomon point out that in order for RHIOs to become a major agent of transformation, effective regulations are required to strengthen the protection of PHI by devising comprehensive privacy and security standards that allow RHIOs to avoid the traps of state-specific regulations.

3.6 Information security issues of e-health:

The emergence of internet technologies has transformed the business model for customer-oriented industries such as retail and the financial services. The healthcare sector is also experiencing a tectonic shift in enablement of healthcare services through internet and mobile technologies such as remote health monitoring, online consultation, e-prescription, e-clinical trials, patient information access and asset tracking.[6][7][8]

With the emergence of e-health networks and HMOs offering web-based services, the future success of e-health is more likely to depend on how effectively patients can securely obtain and manage their information. Recently, several leading technology vendors and consumer-oriented enterprises have established the Liberty Alliance project to promote a common platform for privacy and security in e-commerce, based on the principles of federated identity management (Peyton et al., 2007). This emerging technology framework is being adapted to establish a 'Circle of Trust' (CoT) for cooperating enterprises such as hospitals, pharmacies, labs, and insurers thereby enabling them to offer web-based services to patients. In this framework, personally identifiable information is managed by a designated 'Identity Provider' who provides pseudonymous identities of patients for transactions among partners. Further, an audit service, provided by an independent organisation, logs all transactional requests made by members of CoT, thus enabling:

1 a privacy officer or regulatory agency to validate privacy compliance or investigate allegations of privacy breaches
2 individual patients to verify how their data is being used and challenge data accuracy.

3.7 Information security risks in authorised data disclosure:

In the healthcare sector, it is often necessary to share data across organisational boundaries to support the larger interests of multiple stakeholders as well as agencies involved with public health. However, the release of patient data could entail personally identifying information as well sensitive information that may violate privacy as well cause socio-economic repercussions for patients. Yet such data, when masked for identifying and sensitive information, must maintain the analytic properties to assure statistical inferences, especially when released for epidemiological research.

Disclosure of patient information for research purpose requires that the disclosed data remains consistent with respect to its statistical properties to minimise information. The measurement of information loss, however, depends on potential usages of released data, which is difficult to anticipate at the time of disclosure. For example, some disclosure control methods may alter the multivariate covariance structure of attributes necessary for conducting multivariate regression analyses, while keeping the univariate properties intact. More recently, El Emam and his colleagues extend this research stream by comparative evaluation of some of the most commonly used de-

identification heuristics for disclosure of patient information for public health and health services research, development of new heuristics for such disclosures that ensure balanced trade-off between disclosure risk and information loss, and estimation of population size cut-off at which data suppression could prove fruitful strategy for data disclosure.

3.8 Information integrity in healthcare and adverse effects:

In the healthcare sector, faulty system design features could become a primary internal threat to information security. For example, the integrity of medical records may be compromised by poor alert design. Recent research has shown that excessive alerts may cause 'alert fatigue' leading clinicians to override alerts, and ultimately impacting patient safety.

Recent research shows that CPOE systems, if deployed without extensive knowledge and consideration of extant work practices and information systems, could facilitate 'potential' medical error risks such as:

1 information errors arising from fragmented data and disconnects between CPOE and other information systems.
2 errors arising from the human–machine interfaces that do not reflect conventional behaviour and the decision-making processes of healthcare professionals.

Such adverse findings about CPOE systems are also reflected in the perception of hospital executives. A recent study found that senior managers in hospitals, including pharmacy directors, were satisfied with medication error reducing capabilities of CPOE, but were very concerned about the efficacy of CPOE in paediatric support. Many of these concerns stem from the lack of integration of CPOE with other systems like inventory control systems (Inquilla et al., 2007) or poor design and policy features of the systems (Aarts et al., 2011). This body of research highlights the fact that technology alone cannot meet the ulterior goals of high-quality care. Instead, a balanced approach of investment in technology, processes, people and knowledge base must be considered.

3.9 Financial risk and fraud control:

A significant amount of healthcare expenditures is directly attributable to fraudulent services and billing practices. A recent report from Center for Medicare and Medicaid Services (CMS, 2007) suggests that about $10.8 Billion of payments (3.9% of total $276.2 Billion) did not comply with the norms of Medicare coverage, code billing and payment rules. At a national level, the fraud loss could range from 3% to 10%, suggesting losses due to fraud may be between $68B and $225B on the US $2.26 trillion national health expenditure. According to investigations, healthcare fraud typically involves one of several schemes, including billing for services not rendered, upcoding of services rendered, upcoding of medical items, duplicate claims, unbundling of services, excessive services, medically unnecessary services and referral kickbacks. Johnson (2009) describes the types of medical identity theft, documenting case examples and providing empirical evidence of the vulnerability. In a recent report on the use of health IT to enhance and expand healthcare anti-fraud activities (FORE, 2005), a cross-industry committee examined the potential economic cost/benefit of implementing an Interoperable National Health Information Network (NHIN) and concluded that it could lead to substantial savings. Moreover, such savings could substantially grow with the deployment of intelligent coding tools and analytics for fraud detection.

In developing a framework for statistical monitoring model, Rosenberg (2011) shows that a decision theoretic approach can be used to determine if the NAC rate has substantially changed, warranting further investigation (i.e., additional targeted audits, to manage the NAC rate within acceptable level). The approach makes use of decision rules in the sense that if the expected loss is lower than the expected audit cost, the statistical monitoring model recommends no investigation for the principal diagnosis under review. Payer organisations equipped with such statistical monitoring tools for controlling the NAC rate could direct their resources to other necessary services rather than on expensive audits.

3.10 Regulatory implications to healthcare practice:

A significant body of public policy research, both in medical informatics and in law, also investigates the implications of privacy and security. Much of this work has focused on the legal aspects of EHR and privacy facilitation through technology and policies.

Conclusions

In this paper, we have examined the extant body of knowledge on privacy and security in healthcare, spanning several research domains including privacy concerns among healthcare consumers and providers' perspective of regulatory compliance. Our review indicates that scholars from health informatics, legal and computer science have adopted a multitude of methodologies including design research, qualitative and quantitative research methods to examine various aspects of security and

privacy in the healthcare sector. Information security has drawn significant attention among mainstream information systems scholars, yet there has been relatively little published concerning the unique security challenges found in healthcare. We believe that the increasing importance of information security and the need for managerial insights to these problems offer an exceptional opportunity for debate and cross fertilisation within the IS research community. Certainly, there is a substantial need for new ideas that could guide practitioners through this time of change within the industry.

References

[1] B. C. Neuman and T. Tso, "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications*, Vol. 32, No. 9, pp. 33 – 38, Sept. 1994.

[2] S. Garfinkel, PGP: Pretty Good Privacy, *O'Reilly*, Dec. 1994, ISBN: 1565920988.

[3] D. E. Comer, *Computer Networks and Internets*, 5th Edition, Prentice Hall, Apr. 2008, ISBN: 0136061273.

[4] B. Ramsdell, *S/MIME Version 3 Message Specification*, IETF RFC 2633, Jun. 1999.

[5] Gray,T.,et al(Mar.2002).Network Security Credo[Electronicversion].RetrievedNov.25,2005.

[6] Agrawal, R. and Johnson, C. (2007) 'Securing electronic health records without impeding the flow of information', *International Journal of Medical Informatics*, Vol. 76, Nos. 5–6, pp.471–479.

[7] AHRQ (2007a) *Privacy and Security Solutions for Interoperable Health Information Exchange: Final Implementation Plans*, Report for Agency for Healthcare Research and Quality, and Office of national Coordinator for Health Information Technology.

[8] Al-Nayadi, F. and Abawajy, J.H. (2007) 'An authorization policy management framework for dynamic medical data sharing', *International Conference on Intelligent Pervasive Computing*, Jeju Island, Korea, pp.313–318.