Information Security and Privacy in Healthcare: Current State of Research[1]

Ajit Appari (Ajit.Appari@Tuck.Dartmouth.edu)
And
M. Eric Johnson (M.Eric.Johnson@Tuck.Dartmouth.edu)
Center for Digital Strategies
Tuck School of Business
Dartmouth College, Hanover NH

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.

Keywords: Information Security, Privacy, Healthcare, Research Literature.

August 2008

[1] This research was supported through the Institute for Security Technology Studies at Dartmouth College, under awards 60NANB6D6130 from the U.S. Department of Commerce and U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001. The statements, findings, conclusions, and recommendations are those of the authors and do not necessarily reflect the views of the National Institute of Standards and Technology (NIST), the U.S. Department of Commerce, or U.S. Department of Homeland Security.

1 Introduction

Recent government initiatives envision adoption of a universal electronic health record (EHR) by all health maintenance organizations (HMO) by year 2014 (Goldschmidt 2005). 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 US could potentially save $81B annually by moving to EHR system (Hillestad et al. 2005). Yet information technology (IT) spending in healthcare sector trails that of many other industries, typically in 3-5% of revenue, far behind industries like financial services where closer to 10% are the norm (Bartels 2006). Anecdotal evidences from recent years suggest 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 2007). A recent survey in the United States suggests that 75% of patients are concerned about health Web sites sharing information without their permission (Raman 2007). Possibly this is because medical data disclosure is the second highest reported breach (Hasan and Yurcik 2006).

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.

Since Anderson's seminar work on security in healthcare information systems (Anderson 1996), scholars have examined the information security problem in different ways. 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 one hand, a large body of research focuses on developing technological solutions for ensuring privacy of patients when their information is stored, processed, and shared. On the other hand, several researchers have examined the impact of Health information technology adoption on care quality. Additionally, the enactment of the Health Insurance Portability and

Accountability Act (HIPAA) and emergence of web-based healthcare applications has turned researchers' attention towards patient as well provider perspectives on HIPAA. Surprisingly, very limited attention has been given to the financial risks, especially those arising from medical identity theft and healthcare fraud.

The rest of the paper is structured as follows. First we present a general view of information privacy and security in healthcare, briefly discussing HIPAA and the evolving threat 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.

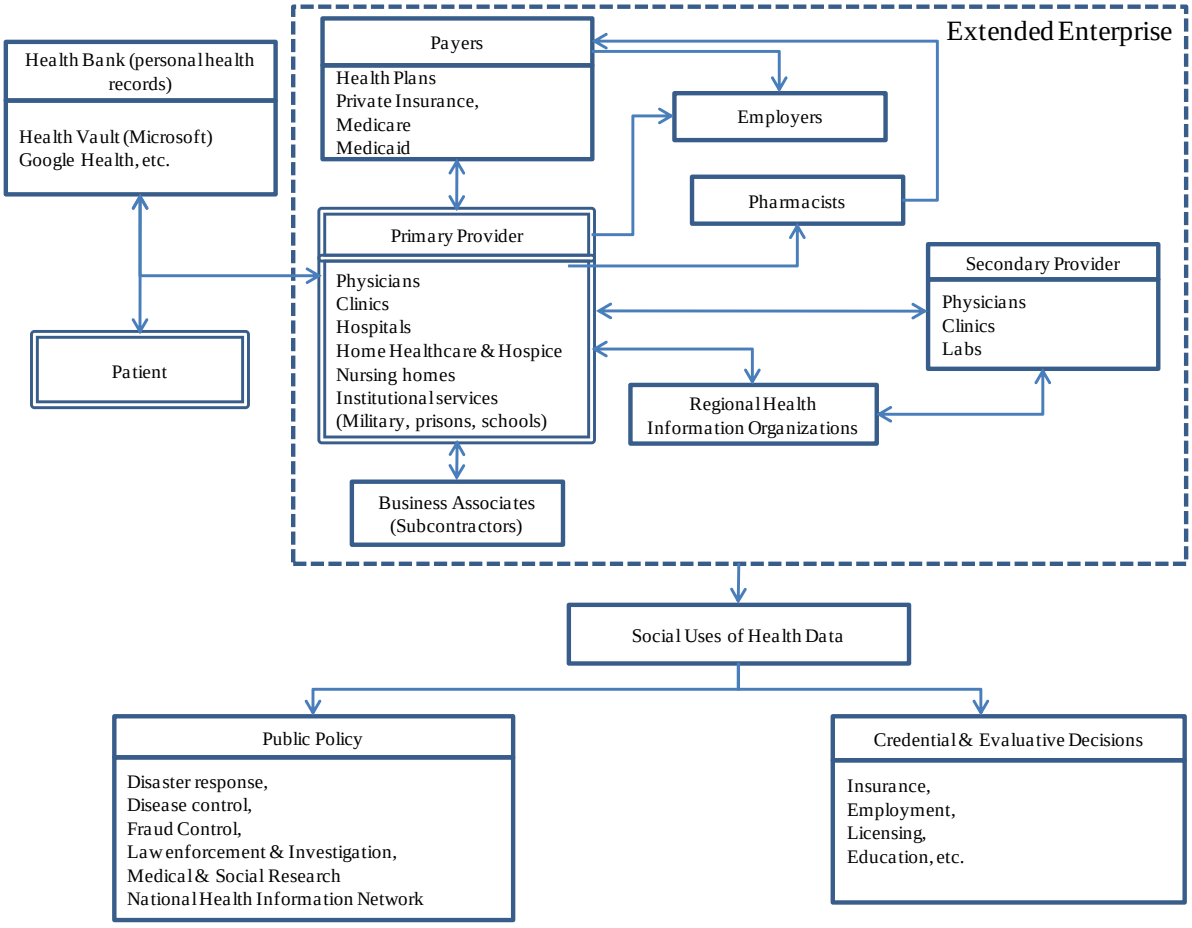
2 Background of Health Information Privacy and Security

Privacy is an underlying governing principle of the patient – physician relationship for effective delivery of healthcare. Patients are required to share information with their physicians to facilitate correct diagnosis and determination of treatment, especially to avoid adverse drug interactions. However patients may refuse to divulge important information in cases of health problems such as psychiatric behavior 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, treatment received, medication history, dietary habits, sexual preference, genetic information, psychological profiles, employment history, income, and physicians' subjective assessments of personality and mental state among others (Mercuri 2004).

The figure 1 shows a typical information flow in the healthcare system. Patient health records could serve a range of purposes apart from diagnosis and treatment provision. For example, information could be used to improve efficiency within healthcare system, drive public policy development and administration at state and federal level, and in the conduct of research to advance medical science (Hodge 2003). A patient's medical records are also shared with payer organizations such as insurance, Medicare or Medicaid to justify payment of services rendered by physicians. Healthcare providers may use records to manage their operations, to assess service quality, and to identify quality improvement opportunities. Furthermore, providers may share health information through a regional

health information organization to facilitate care services. Medical information of patients is also used for common good through federal and state government interventions regarding public health management, hospital accreditation, medical research, and for managing social and welfare systems.

Figure 1: A Graphical View of Information Flow in the Health Care System



2.1 Health Information Privacy Regulations

In the last four decades, the US healthcare industry has undergone revolutionary changes, driven by advances in information technology and legislation such as the 1973 Health Maintenance Organizations Act. As personal health information is digitized, transmitted and mined for effective care provision, new forms of threat to patients' privacy are becoming evident. In view of these emerging threats and the overarching goal of providing cost effective healthcare services to all citizens, several important federal regulations have been enacted including the Privacy and Security Rules under HIPAA (1996) and State Alliance for eHealth (2007).

HIPAA was enacted to reform health insurance practices as a step towards moving to a nationwide electronic health records system and standardizing information transactions. The goal was to reduce costs by simplifying the administrative processes to provide continuity of care services.. The technology component involved in managing health information and necessity of disclosure to third parties has led to stipulations of privacy compliance and provision of security safeguards under HIPAA (Mercury 2004). The Privacy Rule of HIPAA addresses the use and disclosure of a patient's protected health information by healthcare plans, medical providers, and clearinghouses, also referred as "covered entities". By virtue of their contact with patients, covered entities are the primary agents of capturing a patient's health information for a variety of purposes including treatment, payment, managing healthcare operations, medical research, and subcontracting (Choi et al. 2006). The Security Rule of HIPAA requires covered entities to ensure implementation of administrative safeguards in the form of policies and personnel, physical safeguards to information infrastructure, and technical safeguards to monitor and control intra and inter organizational information access (ibid.)

Apart from HIPAA, by 2007, nearly 60 Health IT related laws have been enacted in 34 states, plus the District of Columbia (RTI 2007). Moreover, the US Congress has been considering various new legislation including "Health Information Privacy and Security Act" (US Congress 2007a), "National Health Information Technology and Privacy Advancement Act of 2007" (US Congress 2007b), and "Technologies for Restoring Users' Security and Trust in Health Information Act of 2008" (US Congress 2008). This new legislation is intended to improve the privacy protection offered under previous regulations by creating incentives to de-identify health information for purposes necessary, establishing health information technology and privacy systems, bringing equity to healthcare provision, and increasing private enterprise participation in patient privacy.

2.2 Threats to Information Privacy

Threats to patient privacy and information security could be categorized into two broad areas: (1) Organizational threats that arise from inappropriate access of patient data by either internal agents abusing their privileges or external agents exploiting vulnerability of information systems, and (2) Systemic threats that arise from an agent in the information flow chain exploiting the disclosed data beyond its intended use (NRC 1997).

Organizational Threats: may assume different forms, such as an employee who accesses data without any legitimate need or an outside attacker (hacker) that infiltrates organization's information infrastructure to steal data or render it inoperable. At the outset, these organizational threats could be characterized by four components – motives, resources, accessibility, and technical capability (NRC 1997). Depending on these components, different threats may pose different level of risk to organization requiring different mitigation and prevention strategies. Motives could be both of economic or noneconomic nature. For some, such as insurers, employers, and journalists, patient records may have economic value, while others may have noneconomic motives such as a person involved in romantic relationship. These attackers may have resources ranging from modest financial backing and computing skills to a well-funded infrastructure to threaten a patient as well as the operations of a healthcare organization. The attackers may require different types of access to carry out their exploits, such as access to the site, system authorization, and data authorization (See table 1 for hypothetical examples for level of access). In addition, threats could depend on technical capability of attackers who may be novice or sophisticated programmers. Moreover, with the growing underground cyber economy (Knapp and Boulton 2006), an individual with the intent to acquire data and possessing adequate financial resources may be able to buy services of sophisticated hackers to breach healthcare data.

Recent studies suggest that the broad spectrum of organizational threats could be categorized into five levels, in the increasing order of sophistication (NRC 1997; Rindfleisch 1997):

1. *Accidental disclosure*: healthcare personnel unintentionally disclose patient information to others, e.g. email message sent to wrong address or an information leak through peer-to-peer file sharing.
2. *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 sexually transmitted disease in colleague; or medical personnel accessing potentially embarrassing health information about a celebrity and transmitting to media.
3. *Data breach by insider*: insiders who access patient information and transmit to outsiders for profit or taking revenge on patient.
4. *Data breach by outsider with physical intrusion:* an outsider who enters the physical facility either by coercion or forced entry and gains access to system.

5. *Unauthorized intrusion of network system* : an outsider, including former vengeful employees, patients, or hackers who intrude into organization's network system from outside and gain access to patient information or render the system inoperable.

Table 1: Likely Combinations of Access Privileges in Healthcare Data Breach [source: NRC 1997]

Level of Access	Example
None	Outside Attacker
Site only	Maintenance worker
Site and System	Employee in the billing department who has access to information systems but not to clinical information
Data and System	Vendor or consultant with remote access privileges
Site, System, and Data	Care provider such as doctor or nurse

Systemic Threats: Etzioni (1999), in discussing the '*Limits to Privacy*', makes a strong case that a major threat to patient privacy occurs not from outside of the information flow chain in healthcare industry but from insiders who are legally privileged to access patient information. For example, insurance firms may deny life insurance to patients based on their medical conditions, or an employer having access to employees' medical records may deny promotion, or worse, terminate employment. Patients and /or payer organizations may incur financial losses as a result of malpractices including upcoding of diagnoses, and rendering of medically unnecessary services.

In summary, healthcare information systems could be subjected to security threats from one or more sources including imposter agents, unauthorized use of resources, unauthorized disclosure of information, unauthorized alteration of resources, and unauthorized denial of service (Win et al. 2006). Denial-of-service attacks via Internet worms or viruses, equipment malfunctions arising from file deletion or corrupted data, and the lack of contingency plans pertaining to offsite backup, data restoration procedures, and similar activities may also trigger HIPAA violations (Mercuri 2004).

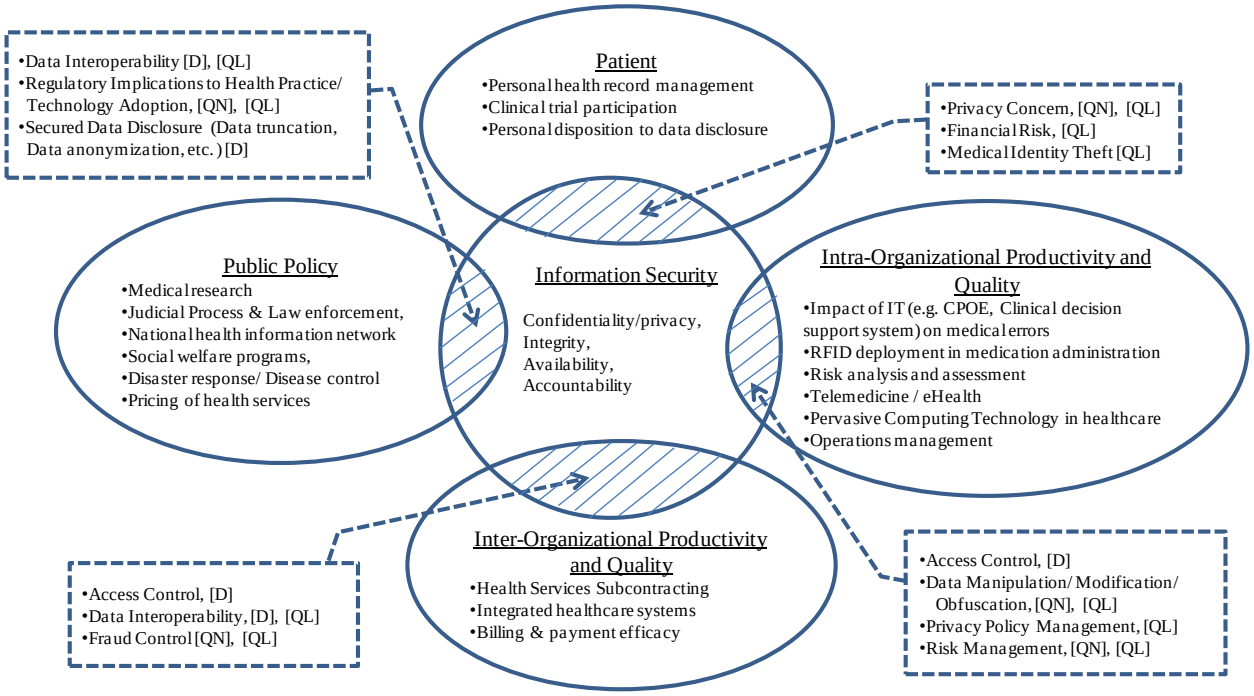
3 State of Information Security Research in Healthcare

In this sections, we present a comprehensive review of information security literature in healthcare sector (refer to appendix 1 for categorization of articles reviewed in this paper). 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. Figure 2 shows the link between many important healthcare research problems and information security. 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. We will use Figure 2 throughout our review to highlight the link between security research and other large streams of research.

It is noteworthy that past research has used diverse range of research methodologies, including design research, qualitative research and quantitative research. Design research focuses on developing artifacts such as models, algorithms, prototypes, and frameworks to solve specific information system problems (Hevner et al. 2004). In healthcare information security research, we find articles focusing on technological solutions for maintaining patients privacy in the wired and wireless network of a provider organization, (authorized) disclosure of patient data for secondary usage such as academic research, and data sharing in a network of providers among others (e.g., Dong and Dulay 2006; Malin 2007; Malin and Arioldi 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, most of the qualitative research centers around impact of HIPAA regulation on healthcare practices (e.g. Ferreira, et al. 2006; Hu, et al. 2006; Terry and Francis 2007). Lastly, healthcare information systems research have adopted several quantitative methods including survey based research, econometric analysis, and statistical modeling among others in the areas of patients' privacy concern, public policy, fraud control, risk management, and impact of health information technology on medical errors (Bansal, et al. 2007; Koppel, et al. 2005; Miller and Tucker 2008, Rosenberg 2001a,b).

Figure 2: Research Domains in the Healthcare Information Security



[D]: Design Research; [QL]: Qualitative Research ; [QN]: Quantitative Research

3.1 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.

This extensive body of research reviewed in Sankar et al. (2003) mostly considered the use of identifiable or potentially identifiable information to other relevant entities including employers, families, and third parties. However, very limited research has examined patients' perception on sharing of anonymized health records, perhaps

with exception of more recent studies that examine patients perception about consent to health information use for other than their own care (Bansal, et al. 2007; Campbell, et al. 2007). Bansal et al. (2007), on the one hand, developed a set of constructs based on utility theory and prospect theory as antecedents of trust formation and privacy concern that impact users' personal disposition to disclose their health information to online health services websites. In particular, this study reported that user's current health status, personality traits, culture, and prior experience with websites and online privacy invasions play a major role in user's trust in the health website and their degree of privacy concerns. On the other hand, Campbell, et al (2007), in a mail based survey with adult patients in England, found that about 28% to 35% of patients are neutral to their health information – such as age, gender, ethnicity, reason for treatment, medical history, personal habits impacting health, type of treatment obtained, side effects of treatment – being used by physicians for other purpose. Only about 5–21% of patients, however, expected to be asked for permission to use their information by their physicians. Similarly only about 10% of the patients expected to be asked for permission if their doctors use their health information for a wide variety of purposes including, combining data with other patients' data to provide better information to future patients, sharing how the treatment is working with other physicians in the hospital, teaching medical professionals, and writing research articles about diseases and treatments.

In another study, Angst, et al. (2006) investigated divergence of perception among patients toward different types of personal health record systems, including paper based, personal computer based, memory devices, portal and networked PHR, which are in the increasing order of technological advancement. The study found that patient's relative perception of privacy and security concern increased with the level of technology, e.g. relative security and privacy concern for networked PHR is twice that of memory device based PHR. Technologically advanced PHR systems were found to be favored by highly educated patients.

3.2 Providers' Perspective of Regulatory Compliance

HIPAA compliance has become a business necessity in healthcare maintenance organizations (HMO). Recently Warkentin et al. (2006) undertook a study to characterize the compliance behavior among administrative staff and medical staff of public as well private-sector healthcare facilities. The authors observed that healthcare professionals at public hospitals have higher self efficacy, i.e. belief in their capability to safeguard and protect patient's

information privacy, compared to their counterparts in private healthcare facilities. Further, on average, administrative staff exhibited higher self efficacy than medical staff across both public and private healthcare facilities. Moreover, the behavioral intent of healthcare professionals, including medical and administrative staff, was positively correlated to self efficacy and perceived organizational support. Another set of studies show that healthcare workers, having access to patient data, are highly concerned about maintaining accuracy of patient records, unauthorized access to patient data, and believe that patient data should not be used for unrelated purposes except for medical research (Baumer, et al. 2000),

Patients' health information plays a major role in conducting medical research for improving healthcare quality. However, disclosure of health information to researchers raises concerns of privacy violations. Regulations such as HIPAA allow healthcare provider organizations 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 nationwide web-based survey of epidemiologists Ness (2007) report that nearly 68% of researchers perceived 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 HIPAA had increased research cost by a great deal, especially due to additional compliance related administrative cost and about 51% of researchers believed HIPAA enforcement lead to inadvertent delays in research. In a critical review of three cases of health research projects, Shen et al. (2006) report that the complexity of consent forms and privacy protection forms, time consuming and cost amplifying procedures often get in the way of patient recruitment. The authors recommend simplifying the language of privacy and consent forms to facilitate easier comprehension by patients. Furthermore, if breach of confidentiality is a primary risk and the quality of the project could be affected from reduced participation, the authors suggest a viable option would be to discard the consent process and instead include a statement on potential use of PHI in Notice of Privacy Practices allowing patients to make choices based on privacy notice. This adverse view of HIPAA is also reflected in lower adoption rate of health information systems such as EMR bolstering the perception that privacy laws may actually have negative effect on the ulterior goals of providing quality care at low cost. Recently, Miller and Tucker (2007) examined data on enactment of state privacy laws regulating health information disclosure across

the US and the adoption rates of EMR They found that hospitals in states with privacy laws were 33% less likely to adopt an EMR system compatible with other neighboring hospitals. However, in states with no privacy laws, they found that a hospital's adoption of EMR may increase the likelihood of neighboring hospital adopting EMR by about 6 percent. Without other incentives, this adverse effect may hinder the federal goal of an interoperable national health network by year 2014.

The quality of administrative capabilities in managing access control to healthcare information systems has an impact on administrative cost, user downtime between administrative events, and the ability of users to perform their roles (Hu et al. 2006). Among various business applications, enterprise resource planning (ERP) systems is often considered as one of major software applications that could streamline the business process of healthcare facilities (Jenkins and Christenson 2001). This is especially true if it can combine patient information and financial information into one complete record, eliminating the need of redundant data entry and facilitating clinical decision making. However, many ERP systems require customization to ensure HIPAA compliance. Pumphrey et al. (2007) recommend that organizations establish comprehensive policies for privacy and security management, and ensure that technology vendors address these policies in the software.

3.3 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).

Despite significant progress in technological solutions to information access control, operationalization remains a major challenge (Lovis, et al. 2007). Healthcare organizations, because of the complex nature of data access for diverse purposes, often give broader access privileges and adopt 'Break the Glass' (BTG) policy to facilitate timely and effective care. Røstad and Edsburg (2006), for example, report that 99% of doctors were given overriding privileges while only 52% required overriding rights on regular basis, the security mechanisms of health information systems were overridden to access 54% of patients' records. Another common pitfall of BTG policy is that such broad-based privileges could be misused by employees. To address these issues Bhatti and Grandison (2007), proposed a privacy management architecture (PRIMA) model that leverages artifacts such as audit logs arising from the actual clinical workflow to infer and construct new privacy protection rules. In particular, PRIMA implements a policy refinement module that periodically examines the access logs and identifies new policy rules using sophisticated data-mining techniques. These audit logs could, as well, be used by privacy officials to determine privacy violations, which in itself is a complex process and often requires merging data from disparate sources (Ferreira, et al. 2006). Unfortunately such data merging may cause potential disclosure of patients' sensitive information to the investigators against the patients' consent. In a related study, Malin and Arioldi (2007) developed a Confidential Audits of Medical Record Access (CAMRA) protocol to ensure privacy of patient's identity during such linking of disparate databases for comprehensive audit purpose without disclosing sensitive information.

In summary, a significant body of research has been developed in the domain of information access control offering solutions to manage data access privileges in healthcare organizations. Yet, scholars (e.g. Ferreira et al. 2006) recognize that access control management is not just a technical solution but requires consideration of work processes, organizational structure and culture to provide effective information security. Effectiveness of access control system, for example, with overriding privileges would very much depend on how the users interact with the

system. To improve the transparency of access control management, hospital systems are even adopting the policy of sharing audit logs with patients, thus enabling them to continually refine access rights on their health records to healthcare professionals (Lovis, et al. 2007).

3.4 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).

Development of fully functional interoperable EHR system remains a major challenge. Recent research has proposed prototype 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 setting (Raghupathi and Kesh 2007). These SOA based EHRs are expected to be scalable to enable inter-enterprise environments such as regional health information organizations (RHIO), and alliance of such RHIOs could lead to national and global health information networks (Raghupathi and Kesh 2007). In a case study based

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. 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).

3.5 Information Security on Web Enabled Healthcare Provision

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 among others (Kalorama 2007). Recent advances in web technology have enabled new approaches to patient information management such as "Banking on Health' or "Health Bank" (Ramsaroop and Ball 2000). The notion of health bank, first conceptualized in Ramsaroop and Ball (2000), is a platform for storage and exchange of patient health records patterned after a personal banking system where consumers could deposit and withdraw information. Recent launches of 'HealthVault' by Microsoft and 'Google Health' by Google are examples of such health banking system. However such web enabled and mobile based services open up a whole gamut of security risks compounding the privacy problem. The interception of personally identifiable information by malicious intruders could jeopardize individual's welfare and may expose to undesired vulnerabilities, social discrimination or economic loss.

A growing body of research is focused on developing mechanisms to address privacy and security concerns related to internet and mobile technology based healthcare applications (e.g. Dong and Dulay 2006; Hung 2005; Peyton et al. 2007; Raman 2007; Zheng et al. 2007). One such is, development of privacy preserving trust negotiation protocol for mobile healthcare systems (Dong and Dulay 2006) that facilitates trust between user devices in compliance with predefined access control and disclosure policies. Mobile devices, especially those possessed by patients, could be electronically tracked leading to unintended exposure of patient's location. Thus to ensure integrity and confidentiality of patient data, direct downloading of a patient's record to a PDA owned by healthcare professional

visiting the patient must be constrained by location or ownership information (Zheng et al. 2007). Advances are made to incorporate device location and/or ownership constraints to strengthen the privacy enabled RBAC system (Hung 2005; Cheng and Hung 2005). In another study, Choudhury and Ray (2007) present a 'cooperative management' methodology for assuring privacy of different stakeholders interacting via web based applications in the healthcare service sector.

With the emergence of e-Health networks and HMOs offering web based services, the future success of e-Health is likely to depend on how effectively patients can obtain and manage their health related information over the web in secure manner. In view of this, 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 ecommerce, based on the principles of federated identity management (Peyton et al. 2007). This emerging technology framework is being adapted to establish 'circle of trust' (CoT) for cooperating enterprises such as hospitals, pharmacies, labs, and insurance providers 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 independent organization logs all transactional requests made by members of CoT, in compliance with privacy regulations, thus enabling (1) a Privacy Officer or regulatory agency to validate privacy compliance or investigate allegations of privacy breaches, and (2) individual patients to verify how their data is being used and challenge data accuracy (ibid).

3.6 Information Security for Authorized Data Disclosure

In healthcare sector, it is often necessary to share data across organizational boundaries to support the larger interests of multiple stakeholders as well as agencies involved with public health. However, the release of patient's data could entail personally identifying information as well sensitive information that may violate privacy as well cause socioeconomic repercussions for patient. 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 (Truta et al. 2004). Advances in technology have led to consolidation of health records

from multiple sources to a single research database which supports researchers engaged in improvement of public health, clinical methods and health services in general.

A significant and growing body of research, building on the theory of statistical disclosure control , offers a diverse range of data masking methodologies and frameworks to minimize or control the disclosure risk of patient information – e.g. global and local recoding (Samarati 2001), micro-aggregation (Domingo-Ferrer and Mateo-Sanz 2002; Domingo-Ferrer et al. 2006), data perturbation (Muralidhar and Sarathy 2005), data swapping (Dalenius and Reiss 1982; Reiss 1984), and data encryption (Chao et al. 2002; Chao et al. 2005) among others, in addition to de-identification or removal of data identifiers (Ohno-Machado, et al. 2004). However, some scholars argue that it is not possible to completely delink patients' identities from their health information for several reasons such as the discovery of errors or irregularity in care provision requires identification of the patient for corrective follow-up care, poor control on research validity and potential frauds if de-identified/anonymized data cannot be traced back to original source, and increase in cost of data maintenance (Behlen and Johnson 1999). More recently, scholars suggested SQL searching mechanisms of encrypted data (Susilo and Win 2007) and attribute protection enhancement to k-anonymity algorithm (Truta and Vinay 2006) to maintain confidentiality of patients during data disclosure for secondary purposes such as medical research. Similarly, set theory is used to build k-unlinkability that could offer protection from intruders who may match publicly available information such as trails of location visits to "re-identify" a patient (Malin 2007). Reidl et al. (2007) devised an innovative architecture for creating a secure pseudonymous linkage between patient and her health record that will allow authorization to approved individuals, including healthcare providers, and relatives, and researchers.

Theoretical advances on data masking in academic research, discussed above, are as well being strengthened contemporaneously with industrial research and technological advances such as Hippocratic database (Agrawal et al. 2002) and Sovereign Information Sharing platform (Agrawal et al. 2003; 2004). Hippocratic database is an integrated suite of technologies that facilitates effective management of information disclosure from patients' health records in compliance with regulatory standards without impeding the lawful flow of information to support activities associated with individual level care provision and public health management (Agrawal and Johnson 2007). These advances have spurred further research on issues concerned with acquisition of privacy preferences

from patients under the aegis of eHealth applications built on Hippocratic database platform, such as complexity and the large number of combinations of data recipients, purposes, and granularities of data (e.g. Hong et al. 2007).

3.7 Information Integrity in Healthcare and Adverse Effects

Information security risks are often interpreted by terms like 'data breach' in mainstream of information systems literature. However one of the key concepts of information security is ensuring data integrity in addition to confidentiality and availability. In healthcare sector, design features of information system 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 shows that excessive alerts may cause "alert fatigue" leading clinicians to override alerts which may be important to patient safety (Sijs et al. 2006). A growing body of research has focused on alert overriding patterns among clinicians using both quantitative and qualitative research methods. Sijs and her colleague reviewed 17 articles related to CPOE and CDSS implementations using *Reason's framework of accident causation* and conclude that the systems with high override rates may result in an increased level of adverse drug events. Three of the studies reviewed with 57–90% overriding rates observed adverse drug events in 2–6% of the overridden alerts (Sijs et al. 2006). Furthermore, the proliferation of IT in health sector has led to prevalence of larger patient data repositories across American hospitals for medical decision making, giving rise to concerns on quality and reliability of patient data for effective medical decision making (Lorence, et al. 2002). In a survey of health information managers across United States, Lorence et al. (2003) discovered that, despite a national mandate to promote and adopt uniform data quality management, about 39% of health information managers indicate their organizations have not adopted adequate timeliness policies to correct errors.

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, and (2) errors arising from the human-machine interface that do not reflect conventional behavior and decision making processes of healthcare professionals (Han, et al. 2005; Koppel, et al. 2005; Walsh, et al. 2006). 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 pediatric 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. 2004). 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.

3.8 Financial Risk and Fraud Control

A significant amount of healthcare expenditures in United States is directly attributable to providers' 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 dollars paid) did not comply with the norms of Medicare coverage, code billing, and payment rules. At 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 (FBI 2007). According to FBI investigations, healthcare fraud could involve several types of 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. In a recent report on the use of health information technology to enhance and expand healthcare anti-fraud activities (FORE 2005), a cross industry national executive committee examined the potential economic cost/ benefit of implementing interoperable EHR based national health information network (NHIN) and concluded that it could lead to substantial savings. Moreover, such net savings could become multifold on deployment of intelligent coding tools, and analytics for fraud detection.

Healthcare Providers document diagnosis using International Classification of Diseases (ICD), which has over 120,000 codes (O'Malley, et al. 2005). This coding system serves various purposes, in addition to classifying morbidity and mortality information, including reimbursement, administration, epidemiology, and health services research. For billing purposes, these ICD codes are grouped at macro level according to Drug Related Group (DRG) coding principles. According to O'Malley, et al. (2005), documentation errors could creep into patients' medical record from different sources as patients proceed through the process of arrival to discharge. For example, these data errors could result from the amount and quality of information at admission, communication quality between patients and clinicians, clinical training and experience, transcription error, training and experience of coders, and

incorrect bundling of codes among others (O'Malley, et al. 2005). In a recent survey study of information managers, Lorence, et al. (2002) reported that about 14% of managers agree that at least 5% of codes are changed by billing departments. This raises a concern on providing high quality health services, especially when health practitioners are becoming dependent on information systems for decision making. In most service delivery settings, dependence on information systems can become challenging if the system's source knowledgebase is of unknown reliability (Lorence, et al. 2002a). Yet, quality improvements in healthcare, in particular from improved data integrity, and timely availability of health history may reduce medical errors, and lessen duplicate tests yielding substantial benefits to payers (Xu 2007).

Information security risks in healthcare have monetary consequences to multiple stakeholders including patients, healthcare organizations, and payers (e.g. insurance). On the one hand, a recent identity theft survey conducted by FTC suggested that in 2005 about 3.7% of consumers were victims of identity theft - 3% of which were medical thefts where perpetrators received medical services using stolen personal information (FTC 2007). On the other hand, General Accounting Office of US estimated that 10% of health expenditure reimbursed by Medicare accounts for healthcare is paid to fraudsters, including identity thieves and fraudulent health service providers (Bolin and Clark 2004; Lafferty 2007). As a result, federal initiatives were taken to establish a *healthcare fraud and abuse program* as part of the HIPAA enactment in 1996. Since then, fraud control units at Center for Medicare and Medicaid Services (CMS) investigate submitted claims and compare them to patients' medical record to identify occurrence of fraud and prosecutes the fraudulent entities. A series of audit based studies have been conducted in the past to identify determinants of healthcare fraud and abuse, in particular observable characteristics of providers/ hospitals and claims associated with fraudulent behavior (Hillman, et al. 1990; Psaty, et al. 1999; Silverman and Skinner 2004; Swedlow, et al. 1992). In particular, Silverman and Skinner (2001) find evidence that upcoding behavior (i.e., the practice of billing for higher charges) at non-profit hospitals is similar to that of for-profit hospitals in the market where for-profit hospitals have a higher share of patient discharge, and for-profit hospitals generally resort to upcoding practices even if they have minority share. More recently, an empirical study by Becker, et al. (2005) concluded that increased expenditure at the Medicare Fraud Control Unit (MFCU) reduced upcoding practices in context of patients diagnosed with illnesses including respiratory infections and pneumonia, circulatory system disorders, kidney disorders, diabetes and nutritional/metabolic disorders.

In a detailed investigation of why fraud plagues America's healthcare system, Sparrow (1996; 1998) argued that fraud control is a very complex endeavor and that most insurers have failed to measure the magnitude of the problem. Currently, organizations use various approaches including automated claims auditing, manual examination or audits of submitted claims, prepayment medical review and post-payment utilization review (Sparrow 1998). Among them, they found that post-payment utilization review is the major tool (ibid) used by payer organizations. Using that tool, sampled medical records associated with episodes of inpatient claims are audited to detect fraudulent behavior of healthcare providers - an expensive undertaking for payer organizations (Rosenberg 2001). A growing body of research in the fraud control area is exclusively focusing on usage of readily available data from Universal Billing Form version 82 (UB82) to explicate changes in the rate of Non-Acceptable inpatient hospital Claims (NAC). This approach is an outgrowth of statistical quality control (Rosenberg 1998; Rosenberg, et al. 1999; Rosenberg and Griffith 2000; Rosenberg 2001a,b; Rosenberg, et al. 2001). This stream of research seeks to develop statistical control models for managing the NAC rate and supporting the traditional manual audits of claims. In particular, such statistical systems that monitor all submitted claims instead of medical records sampled for audit, could be used to monitor subgroups of claims to detect if the NAC rate has changed or to determine which individual claims should be audited. Further the NAC rates are established for each diagnosis related groups (DRG) using a Bayesian logistic regression model on the audited claims data stratified by DRGs, i.e. medical records and UB82 data. For each principal diagnosis or DRG, this Bayesian model predicts the probability of a claim being NAC using audit data as a function of several explanatory variables including sex, age, length of stay, emergency admission type, urgent admission type, and medical type of service thus establishing *a priori* distribution of NAC rate. Subsequently, the *posterior* distribution is generated by considering all claims submitted during an interval between two planned consecutive audits. In developing a framework for statistical monitoring model, Rosenberg (2001a) 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). In particular, 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 organizations equipped with such statistical monitoring tools for controlling the NAC rate could direct their resources to other necessary services rather than on expensive audits (Rosenberg 2001b).

3.9 Regulatory Implication to Healthcare Practice

A significant body of research both in medical informatics and 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 (Applebaum 2002; Cate 2002; Epstein 2002; Finne 1996; Hodge et al. 1999; Hyman 2002; Magnusson 2004; Mandl et al. 2001; Rothstein et al. 2007; Terry and Francis 2007; Tyler 2001), privacy of third party information related to human subjects in medical research (Lounsbury et al. 2007), tradeoff between personal privacy and population safety (Baker 2006; Gostin et al. 2001; Gostin and Hodge 2002; Hodge 2006; Hodge and Gostin 2004), and medical error and risk information mining (Kuno et al. 2007; Tsumoto et al. 2007).

Applebaum (2002) reviewed the ethical and legal underpinnings of medical privacy governing the patient-doctor relationship, including some of the empirical data derived from third party surveys such as the Gallup survey, California Health Foundation, and academic research (e.g., Kraemer and Gesten (1998)). Applebaum concluded that HIPAA is less friendly, especially in the psychiatric treatment, to medical privacy and that the onus lies with the discretionary interpretation of physicians. Rothstein, et al. (2007) presents analysis of the magnitude of information disclosure that could be permitted under HIPAA. Even by considering a limited set of contexts (for example employment entrance examinations, individual life insurance applications, individual long-term care insurance application, disability insurance claims, automobile insurance claims) Rothstein et al (2007) projected that, on average, 25 millions health records are lawfully disclosed. In view of such staggering disclosures (especially when the recipients may get more information about an individual than necessary for decision making) Rothsetin et al (2007) argued for development of "contextual access criteria" that could be deployed throughout the national health information network to limit the scope of disclosure. In addition concerted efforts need to be made to provide privacy safeguards based on fair information practices, incorporate industry wide security protection, and establish a national data protection authority (Hodge, et al. 1999).

In psychosocial and health-behavioral research, medical researchers often collect information on "third parties" who are related to research participants. Building upon recommendations by Office for Human Research Protections (OHRP) and Botkin (2001), Lounsbury, et al. (2007) propose a rule set that could be adopted by Institutional Review Boards (IRBs) in deciding when informed consent for third party research could be waived. To balance the

conflicting needs of individuals' privacy and public health maintenance, HIPAA grants disclosure privileges to 'covered entities' without individual authorization. Yet the onus of justifying access to patient information lies with public health authorities (Hodge and Gostin 2004). The advocates of public health argue that "privacy interests should be strongest where they matter most to the individual … and communal interests should be maximized where they are likely to achieve the greatest public good…" (Hodge and Gostin 2004: p 676).

3.10 Information Security Risk Management

Information security risk arising from data dissemination for purposes other than care provision has significant ramifications to patients' identity and welfare. To protect the confidentiality of patients, the data owners must satisfy two opposing objectives, namely the privacy of individuals and usability of released data (Winkler 2004). These two objectives are generally referred to as – disclosure risk and information loss. A growing body of research focusing on developing data disclosure methods, and evaluation of such methods, employ a variety of measures for disclosure risk and information loss (e.g. Truta, et al. 2003a,b; Truta, et al. 2004; Winkler 2004). For example, Truta et al. (2003a) defines a set of disclosure risk measures, in particular *minimal disclosure risk, maximal disclosure risk, and weighted disclosure risk*, which could be used for a wider combination of methods adopted for disclosing patients' health information. These disclosure risk measures are derived for estimating the overall quantum of disclosure risk for a given disclosure request under two different disclosing methods – (1) identifier removal method in which personally identifiable are extricated in the released dataset, and (2) sampling and microaggregation methods in any order on the initially masked data obtained from previous method. The authors, in deriving these three measures, make assumption about the extent of prior knowledge an intruder may have from external sources. In another study, Truta et al. (2004a) considered sampling based data disclosure method to assess its performance with respect to above three risk measures. More recently, Truta and his colleagues extended this line of research by considering new dimensions in data disclosure, in particular, potential utility for intruders and ordered relation of attributes that could be exploited by intruders (Truta et al. 2004b).

Disclosure of patient information for research purpose requires that the disclosed data remains consistent with respect to its statistical properties to minimize information. The measurement of information loss, however, depends on potential usages of released data, which is difficult to anticipate at the time of disclosure (Domingo-Ferrer et al.

2001). 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. Truta et al. (2003b) propose modifications to information loss measures presented in Domingo-Ferrer at el (2001) taking into account peculiarity of health data.

Information security risks to health information systems, as discussed earlier in section 2, could arise from different sources. Managing information security risks is a complex process and requires investments in organizational resources and multipronged approaches such as Bayesian network analysis (Maglogiannis and Zafiropoulos 2006), elicitation of user's privacy valuation using experimental economics (Poindexter, et al. 2006), operationally critical threat, asset, and vulnerability evaluation (OCATVE) approach (Alberts and Dorofee 2003), predictive Bayesian approach based risk analysis (Aven and Eidesen 2007), and information security insurance contract (Lambrinoudakis et al. 2005) among others.

4 New Directions for Information Security and Privacy Research

The American healthcare delivery system has transformed over the past century from a patient–physician dyadic relationship into a complex network linking patients to multiple stakeholder. Information technology advances and their adoption into healthcare industry are likely to improve healthcare provision quality, reduce healthcare cost, and advance the medical science. However, this transformation has increased the potential for information security risk and privacy violation. It is estimated that healthcare fraud comprises about 10% of total health expenditure in United States (Dixon 2006). Moreover, with growing digitization of health records, medical identity theft has become a larger looming issue, costing payers and patients. Anecdotal evidence suggests that major threats to patient privacy are internal factors, not external (Wall Street Journal 2008).

In this survey of information security research in healthcare sector we reviewed extant body of knowledge spanning nine broad themes of research domains – threats to information privacy, a definitional research area; privacy concerns among healthcare consumers; healthcare professionals' concern of regulatory compliance; financial risk; information access control; information security risks to eHealth; information security for authorized data disclosure; information reliability in healthcare and adverse effects; and information security risk measurement and management. This review indicates that scholars from health informatics, legal, and computer science disciplines

have adopted a multitude of methodologies including design research, qualitative, and quantitative research methods to examine various aspects of information security and privacy in the healthcare sector. Information security per se has drawn significant attention among mainstream information systems scholars, yet very little has been published in the mainstream information systems journals on information security in healthcare. Next we highlight some of the potential research directions that could enhance this research area.

Threats to information privacy: extant knowledgebase on information security risks identify different types of threats to privacy and security of health information. Future research may focus on characterizing these threats based on organizational contexts, which may help practitioners in developing effective information security risk monitoring and management policies.

Privacy concerns among healthcare consumers: with increasing reliance on web based systems for managing health information, and deployment of health banks privacy concerns of healthcare consumers has been brought to the forefront. Recent research in this area has often focused on restricted user bases, such as students. Future research may explore the variance of privacy preferences in the context of online systems among broader range of users including working population, and senior citizens. A deeper understanding of factors influencing healthcare consumers' willingness to disclose personal information would enable enhancing the adoption of eHealth.

Healthcare professionals' concern of regulatory compliance: with increased regulation on data use and control, managers are increasing concerned with compliance. Research on employee security hygiene in complex healthcare environments is clearly needed.

Financial risk: Information security failures could also lead to financial losses to various stakeholders including patients, providers, and payers arising from fraudulent care and drug charges by organized criminals (Ball et al. 2003), the sale of medical identities to illegal immigrants (Messmer 2008), and fraudulent billing for services never received leading to erroneous health records and potential harm to patients (Dixon 2006). Aside such anecdotal evidences, a systematic study of financial risk is in order to guide information security policy development and inform health maintenance organizations as they move toward wider adoption of electronic health records systems.

Information access control: current research on information access has primarily focused on technological solutions to the problem. Very little, if any, econometric and economic research is pursued that may offer prescriptive

guidelines for decision making. Healthcare organizations require investing on information security measures, such as access control systems, intrusion detection systems, policies, and personnel among others. Failure of such information security systems may severe business continuity and may diminish operating efficiency. The myriad of information systems in hospitals are complex and highly interdependent.. With the emergence of ubiquitous access to patient information using mobile technologies in provider organizations (Abaraham, et al. 2008) this complexity is bound to rise. Recently, Zhao and Johnson (2008) modeled, using game theoretic approach, the information access governance problem in a data oriented enterprise to study the impact of incentives coupled with auditing to determine optimal levels of access. Establishing and revising access control policies in hospital environments, due to the multitude of roles, interdependent information systems, and dynamic nature of role assignment, is an expensive endeavor. Future research could examine the information governance problem accounting for the peculiarities of a healthcare organization. Furthermore, research could develop insights into the characteristics of interdependency between business processes enabled by information systems, and how such network of processes could be unduly affected by information security failures. In our extensive review of literature, we find only empirical study reporting on access privilege provision and actual usage for a European hospital. Similar studies in the context of American hospitals are called for to inform the research and practice on the usage of information access privileges and overriding habits.

Information security to eHealth: over the years healthcare sector has experienced a significant growth in use of mobile health devices and web based applications. Contemporaneously, information security research has focused on development of frameworks, and protocols to address security issues in eHealth environment. Future research may examine effectiveness of these frameworks and protocols on operational efficiency of healthcare providers and consumer satisfaction.

Information security for authorized data disclosure: advocates of public health argue that "privacy interests should be strongest where they matter most to the individual … and communal interests should be maximized where they are likely to achieve the greatest public good …" (Hodge and Gostin 2004, p 676). In the past, research has focused on developing theoretical solutions for secure data disclosure. However, every healthcare provider may not deploy state-of-the-art technology, incorporated with most recent algorithms, to disclose data for secondary purposes.

Understanding the operational effectiveness of data disclosure technology from the field may help hospital administration in refining disclosure policies, as well choosing appropriate data disclosure technology solutions.

Information integrity in healthcare: past research has mainly examined the impact of investment in health information technology on medical error for single instantiation of system deployment. Understanding both the economics and effectiveness of security within the context of care quality is a potentially fruitful area of research. Future research is needed to span large number of CPOE installations, both at regional and national level, to characterize the impact of such system on information integrity leading to medical errors. Such studies could consider explicating the influence of several factors such as hospital characteristics, drug safety alert overriding behavior, false alerts due to inadequacy of knowledge base (clinical decision support system), incomplete or erroneous patient record, workflow interruptions or delay, among others. Further, as in Schmidek and Weeks (2005), which examined correlation between adverse events reported prior to during 1992- 2000 and tort claims by patients of Veterans Health Administration, future studies could examine relationship between adverse events arising from information integrity and tort claims in the general population served by HMOs.

We hope that this review and proposed directions for future research will induce a new line of research offering valuable insights to decision makers.

BIBLIOGRAPHY

1. Aarts, J., Doorewood, H., Berg, M. (2004) "Understanding Implementation: The Case of a Computerized Physician Order Entry System in a Large Dutch University Medical Center," *Journal of the American Medical Informatics Association*, col. 11, pp 207-216,

2. 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,

3. Agrawal , R., Kiernan, J., Srikant, R., Xu, Y. (2002) "Hippocratic Databases," *International Conference on Very Large Databases*, Hong Kong, China, August

4. Agrawal, R., and Johnson, C. (2007) "Securing Electronic Health Records Without Impeding the Flow of Information," *International Journal of Medical Informatics*, vol. 76, no. 5-6, pp 471 – 479

5. Agrawal, R., Asonov, D., baliga, P., Liang, L., Porst, B., Srikant, R. (2004) "A Reusable Platform for Building Sovereign Information Sharing Applications," *Workshop on Database in Virtual Organizations*

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

7. Alberts, CJ, Dorofee, A. (2002) *Managing Information Security Risks: An OCTAVE Approach*, Boston: Addison Wesley Publications

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*, pp. 313 – 318

9. Anderson, R.J. "Security in Clinical Information Systems" University of Cambridge, 1996

10. Angst, C.M., Agrawal, R., and Downing, J. (2006) "An Empirical Examination of the Importance of Defining the PHR for Research and for Practice," Robert H. Smith School Research Paper No. RHS-06-011 Available at SSRN: http://ssrn.com/abstract=904611

11. Applebaum, P.S. (2002) "Privacy in Psychiatric Treatment: Threats and Response," *American Journal of Psychiatry*, vol. 159, pp 1809-1818

12. Aven, T., Eidesen, K. (2007) "A Predictive Bayesian Approach to Risk Analysis in Health Care," *BMC Medical Research Methodology*, vol. 7, no. 38

13. Baker, D.B. (2006) "Privacy and Security in Public Health: Maintaining the Delicate Balance between Personal Privacy and Population Safety," *Computer Security Applications Conference*

14. Baker, W.H., Rees, L.P., Tippett, P.S. (2007) "Necessary Measures: Metric-Driven Information Security Risk Assessment and Decision Making," *Communications of the ACM*, vol. 50, no. 10, pp 101-106,

15. Ball, E., Chadwick, D.W., Mundy, D. (2003) "Patient Privacy in Electronic Prescription Transfer," *IEEE Security & Privacy*, pp 77 – 80,

16. Bansal, G., Zaheid, F.,M., Gefen, D. (2007) "The Impact of Personal Dispositions on Privacy and Trust in Disclosing Health Information Online," *Americas Conference on Information Systems*

17. Bartels, A. (2006) "US IT Spending Benchmarks for 2006," Forrester Research Report,

18. Baumer, D. L., Earp, J. B., & Payton, F. C. (2000) "Privacy of medical records: IT implications of HIPAA", *ACM Computers and Society*, vol. 30, no. 4, pp 40–47.

19. Becker, D., Kessler, D., McClellan, M. (2005) "Detecting Medicine Abuse," *Journal of Health Economics*, vol. 24, pp 189-201,

20. 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

21. Bhatti, R., and Grandison, T. (2007) "Towards Improved Security Policy Coverage in Healthcare Using Policy Refinement," in Jonker, W., and Petkovic, M. (Eds.) SDM 2007, Lecture Notes in Computer Sciences 4721, pp 158 – 173

22. Blobel, B. (2004) "Authorization and Access control for Electronic Health Record Systems," *International Journal of Medical Informatics*, vol. 73, pp 251-257

23. Bolin, J.N., Clark, L.S. (2004) "Avoiding Charges of Fraud and Abuse: Developing and Implementing an Effective Compliance Program," *JONA*, vol. 34, no. 12, pp 546-550

24. Botkin, J. R. (2001) "Protecting the Privacy of Family Members in Survey and Pedigree Research," *Journal of the American Medical Association*, vol. 285, no. 2, pp. 207–211

25. Brailer, D.J. (2005) "Interoperability: The Key to the Future Health Care System," *Health Affairs*

26. Campbell, B., Thomson, H., Slater, J., Coward, C., Wyatt, K., and Sweeney, K.(2007) "Extracting Information from Hospital Records: What Patients Think About Consent," *Quality and Safety in Healthcare*, vol. 16, no. 6, pp 404–408

27. Cate, F.H. (2002) "Principles for Protecting Privacy," *Cato Journal*, vol. 22, no. 1, pp 33-57

28. Catley, C., Petriu, D. C., and Frize, M. (2004) "Software Performance Engineering of a Web Service-Based Clinical Decision Support Infrastructure," *Proceedings of WOSP'04*, pp. 130-138

29. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004) "A Model for Evaluating IT Security Investments," *Communications of the ACM*, vol. 47, no. 7, pp 87-92

30. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2005) "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research*, vol. 16, no. 1, pp. 28-46

31. Chao HM, Hsu CM, Miaou S.G. (2002) "A Data Hiding Technique with Authentication, Integration, and Confidentiality for Electronic Patient Records," *IEEE Transactions on Information Technology in Biomedicine*, vol. 6, pp 46 – 53

32. Chao, H., Twu, S., and Hsu, C. (2005) "A Patient-Identity Security Mechanism for Electronic Medical Records During Transit and At Rest," *Medical Informatics and the Internet in Medicine*, vol. 30, no. 3, pp 227 – 240

33. Cheng, V.S.Y., and hung, P.C.K. (2005) "Towards an Integrated Privacy Framework for HIPAA-Compliant Web Services," *IEEE International Conference on E-Commerce Technology*

34. Choi, Y.B., Capitan, K.E., Krause, J.S., and Streeper, M.M. (2006) "Challenges Associated with Privacy in Healthcare Industry: Implementation of HIPAA and Security Rules," *Journal of Medical Systems*, vol. 30, no. 1, pp57–64

35. Choudhury, A., and Ray, P. (2007) "Privacy Management in e-Health," Proceedings of IEEE Healthcom,

36. CMS (2007) "Improper Medicare Fee-For-Service Payments Report - November 2007 Report", last accessed on June 6, 2008 https://www.cms.hhs.gov/apps/er_report/index.asp

37. Covington, M.J., Moyer, M.J., and Ahamad, M. (2000) "Generalized Role-Based Access Control for Securing Future Applications," *National Information Systems Security Conference*, Baltimore, MD

38. 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

39. Dimitropoulos, L.L. (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*

40. Dimitropoulos, L.L. (2007b) "Privacy and Security Solutions for Interoperable Health Information Exchange: Nationwide Summary," *report for Agency for Healthcare Research and Quality, and Office of national Coordinator for Health Information Technology*

41. Dixon, P. (2006) "Medical Identity Theft: The Information Crime that Can Kill You," The World Privacy Forum Report

42. Dogac, A., Namli, T., Okcan, A., Laleci, G., Kabak, Y., Eichelberg, M. (2006) "Key Issues of Technical Interoperability Solutions in eHealth"

43. Domingo-Ferrer, J., Martinez-Balliste, A., Mateo-Sanz, J., Sebe, F. (2006) "Efficient Multivariate Data-Oriented Microaggregation," *The Very large Data Base Journal*, vol. 15, pp 355-369

44. Domingo-Ferrer, J., Mateo-Sanz, J., (2002) "Practical Data-Oriented Microaggregation for Statistical Disclosure Control," *IEEE Transactions on Knowledge and Data Engineering*, vol.14, no.1, 189-201

45. Domingo-Ferrer, J., Torra, V. (2001) A Quantitative Comparison of Disclosure Control Methods for Microdata," In: Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies, Doyle P., Lane J.I., Theeuwes J. J. M., Zayatz, L. (eds.), pp. 111–134

46. Dong, C., and Dulay, N. (2006) "Privacy Preserving Trust Negotiation for Pervasive Healthcare," *Proceedings of Pervasive health Conferences and Workshops*

47. Eichelberg, M., aden, T., Riesmeier, J., Dogac, A., laleci, G. (2005) "A Survey and Analysis of Electronic Healthcare Record Standards," *ACM Computing Survey*, vol. 37, no. 4, pp 277-315,

48. Epstein, R.A. (2002) "HIPAA on Privacy: Its Unintended and Intended Consequences," *Cato Journal*, vol. 22, no.1, pp 13-31

49. Estrella, F., McClatchey, R., Rogulin, D., Amendolia, R., and Solomonides, T. (2004) "A Service-Based Approach for Managing Mammography Data," *Proceedings of the 11th World Congress on Medical Informatics* (MedInfo'04), September 2004, San Francisco, USA.

50. Etzioni, A. (1999) *The Limits of Privacy*, Basic Books, New York,

51. FBI, (2007) "Financial Crime Report to the Public Fiscal Year 2007,", last accessed on June 18, 2008, http://www.fbi.gov/publications/financial/fcs_report2007/financial_crime_2007.htm

52. Ferraiolo, D.F., and Kuhn, D.R. (1992) "Role Based Access Control" *Nat'l Computer Security Conference*

53. Ferreira, A. Correia, R., Antunes, L., Palhares, E., Farinha, P., and Costa-Periera, A. (2006) "How to Break Access Control in a Controlled Manner," *IEEE Symposium on Computer-Based Medical Systems*

54. Finne, T. (1996) "The Information Security Chain in a Company," *Computers & Security*, vol. 15, pp 297-316

55. FORE - Foundation of Research and Education (2005) "Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities,"

56. FTC – Federal Trade Commission (2007) "2006 Identity Theft Report," last accessed on June 18, 2008, http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

57. Gallaher, M.P., O'Connor, A.C., and Kropp, B. (2002) "The Economic Impact of Role-Based Access Control," National Institute of Standards and Technology Report

58. Goldschmidt, P.G., (2005) "HIT and MIS: Implications of Health Information Technology and Medical Information Systems," *Communications of the ACM*, vol. 48, no.10, pp 69-74

59. 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

60. Gostin, L.O., Hodge, J.G., (2002) "Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule," *Minnesota Law Review*, vol.86, pp 1439-1449

61. Gostin, L.O., Hodge, J.G., Valdiserri, R.O. (2001) "Informational Privacy and the Public's Health: The Model State Public Privacy Act," *American Journal of Public Health*, vol.91, no.9, pp 1388-1392

62. Han, Y.Y., Carcillo, J.A., Venkatraman, S.T., Clark, R.S.B., Watson, S., Nguyen, T.C., Bayir., H. and Orr, R.A. (2005) "Unexpected Increased Mortality After Implementation of a Commercially Sold Computerized Physician Order Entry System," *Pediatrics*, vol.116, no.6, pp 1506-1512

63. Hasan, R., and Yurcik, W. (2006) "A Statistical Analysis of Disclosed Storage Security Breaches," *ACM workshop on Storage security and survivability*

64. Health Privacy Project, (2007) "Health Privacy Stories," http://www.healthprivacy.org

65. Hevner, A., March, S.T., Park, J., and Ram, S. (2004) "Design Science Research in Information Systems," *MIS Quarterly*, vol.28, no.1, pp 75-106

66. Hillestad , R., Bigelow , J., Bower, A., Girosi, F., Meili, R., Scoville, R. and Taylor, R. (2005) "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs," *Health Affairs*, vol.24, no.5, pp.1103-1117

67. Hillman, B.J., Joseph, C.A., Mabry,M.R., Sunshine, J.H., Kennedy, S.D., Noether,M. (1990) "Frequency and Costs of Diagnostic Imaging in Office Practice—A Comparison of Self-Referring and Radiologist-Referring Physicians," *New England Journal of Medicine*, vol.323, no.23, 1604–1608

68. Hodge, J.G. (2003) "Health Information Privacy and Public Health," *Journal of Law, Medicine & Ethics*, vol.31, no.4, pp 663-671

69. Hodge, J.G. (2006) "The Legal and Ethical Fiction of 'Pure' Confidentiality," *The American Journal of Bioethics*, vol.6, no.2, pp 21-22

70. Hodge, J.G., Gostin, L.O. (2004) "Challenging Themes in American Health Information Privacy and the Public's Health: Historical and Modern Assessments," *Journal of Law, Medicine & Ethics*, vol.32, no.4, pp 670-679

71. Hodge, J.G., Gostin, L.O., Jacobbson, P.D. (1999) "Legal Issues Concerning Health Information: Privacy, Quality, and Liability," *Journal of American Medical Association*, vol.282-15, pp 1466-1471

72. Hong, Y., Lu,S., Liu, Q., Wang, L., and Dssouli, R. (2007) "A Hierarchical Approach to the Specification of Privacy Preferences," *International Conference on Innovations in Information Technology*

73. Hu, V.C., Ferraiolo, D.F., Kuhn, D.R. (2006) "Assessment of Access Control Systems," NIST Report 7316

74. Hung, P.C.K. (2004) "Towards a Privacy Access Control Model for e-Healthcare Services," *Proceedings of Annual Conference on Privacy, Security and Trust*

75. Hyman, D.A. (2002) "HIPAA and Health Care Fraud: An Empirical Perspective," *Cato Journal*, vol.22, no.1, pp 151-178

76. Inquilla, C.C., Szeinbach, S., Seoane-Vaquez, E., and kappeler, K.H. (2007) "Pharmacists' Perceptions of Computerized Prescriber Order Entry Systems," *American Journal of Health system Pharmacy*, vol.64, pp 1626-1632

77. Jenkins, E.K., and Christenson, E. (2001) "ERP Systems Can Streamline Healthcare Business Functions," *Healthcare Financial Management*, vol.55, no.5, pp 48-52

78. Kaiser, J. (2006) "Patient Privacy: Rule to Protect Records may Doom Long-Term Heart Study," *Science*, vol.311, no.5767, pp 1547-1548

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

80. Kalorama Information (a division of MarketResearch.com) (2007) "Wireless Opportunities in Healthcare"

81. Khansa, L. and Liginlal, D. (2007) "Valuing the Flexibility of Investing in Security Process Innovations," *European Journal of Operational Research*, forthcoming

82. Knapp, K.J., and Boulton, W.R. (2006) “Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments,” *Information Systems Management*, vol.23, no.2, pp 76-87

83. Koppel R, Metlay JP, Cohen A, Abaluck, B., Localio, A.R., Kimmel, S.E., and Strom, B.L. (2005) "Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors," *Journal of American Medical Association*, vol.293, no.10, pp 1197-1203

84. Kumar, V., Telang, R., and Mukhopadhyay T. (2007) “Optimally Securing Interconnected Information Systems and Assets,” *Workshop on the Economics of Information Security*

85. Kuno, E., Hadley, T.R., Rothbard, A.B. (2007) “Costs of Implementing a Computerized Prescription System in a Public Mental Health Agency,” *Psychiatric Services*, vol.58, no.10, pp 1351-1353

86. Lambrinoudaki, C., Gritzalis, S., Hatzopoulos, P., Yannacopoulos, A.N., Katsikas, S. (2005) "A Formal Model for Pricing Information Systems Insurance Contracts," *Computer Standards & Interfaces*, vol.27, pp 521–532

87. Li, N., and Tripunitara, M.V. (2006) “Security Analysis in Role-Based Access Control,” *ACM Transactions on Information and System Security*, vol.9, no.4, pp 391-420

88. Lorence, D.P., Richards, M. (2002) "Variation in Coding Influence Across the USA," *Journal of Management in Medicine*, vol.16, no.6, pp 422-435

89. Lorence, D.P., Spink, A., Jameson, R. (2002b) "Assessing Managed Care Market Variation in Reports of Coding Accuracy" *Managed Care Quarterly*, vol.10, no.4, pp 15-25

90. Lorence, D.P., Spink, A., Jameson, R. (2002a) "Information in Medical Decision Making: How Consistent Is Our Management?" *Medical Decision Making*, vol.22, pp 514-521

91. Lounsbury, D.W., Reynolds, T.C., Rapkin, B.D., Robson, M.E., Ostroff, J. (2007) “Protecting the Privacy of Third-Party Information: Recommendations for Social and Behavioral Health Researchers,” *Social Sciences & Medicine*, vol.64, pp 213-222

92. Lovis, C., Spahni, S., Cassoni, N., and Geissbuhler, A. (2007) “Comprehensive Management of the Access to Electronic Patient Record: Toward Trans-Institutional Networks,” *International Journal of Medical Informatics*, 76, pp 466 – 470

93. Maglogiannis, I., Zafiropoulos, E. (2006) "Modeling Risk in Distributed Healthcare Information Systems," EMBS Annual International Conference

94. Magnusson, R.S. (2004) “The Changing Legal and Conceptual Shape of Health Care Privacy,” *Journal of Law, Medicine & Ethics*, vol.32, no.4, pp 680-691

95. Mailn, B. (2007) “A Computational Model to Protect Patient-Data from Location-based Re-Identification,” *Artificial Intelligence in Medicine*, vol.40, pp 223-239

96. Malin, B., and Airoldi, E. (2007) “Confidentiality Preserving Audits of Electronic Medical Record Access,” *Proceedings of the 12th World Congress on Health (Medical) Informatics - MedInfo*, Brisbane, Australia

97. Mandle, K.D., Szolovits, P., Kohane, I.S. (2001) “Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private,” *British Medical Journal*, vol.322, pp 283-285

98. Mercuri, R.T. (2004) “The HIPAA-potamus in Health Care Data Security,” *Communications of the ACM*, vol.47, no.7

99. Messmer, Ellen (2008) “Health care organizations see cyber attacks as growing threat,” *Network World*

100. Miller, A.R., and Tucker, C.E. (2007) "Privacy, Network Effects and Electronic Medical Record Technology Adoption," *Proceedings of the Sixth Workshop on the Economics of Information Security*, Carnegie Mellon

101. Motta, G.H.B., and Furuie, S.S. (2003) "A Contextual Role-Based Access Control Authorization Model for Electronic Patient Record," *IEEE Transactions on Information Technology in Biomedicine*, vol.7, no.3

102. Muralidhar, K., and Sarathy, R. (2005) "An enhanced Data Perturbation Approach for Small Data Sets," *Decision Sciences*, vol.36, no.3, 513-529

103. Myers, M.D. (1997) "Qualitative Research in Information Systems," *MISQ Quarterly*, *vol.*21, no.2, pp 241 – 242

104. Nepal, S., Zic, J., Jaccard, F., Kraehenbuehl, G. (2006) "A Tag-Based Model for Privacy Preserving Medical Applications," in *Current Trends in Database Technology – EDBT Workshop*, Grust et al. (Eds.), pp 433-444

105. Ness, R.B. (2007) "Influence of the HIPAA Privacy Rule on Health Research," *Journal of American Medical Association*, vol.298, no.18, pp 2164-2170

106. NRC National Research Council (1997) "For the Record: Protecting Electronic Health Information"

107. O'Keefe, C.M., Greenfield, P., and Goodchild, A. (2005) "A Decentralized Approach to Electronic Consent and Health Information Access Control," *Journal of Research and Practice in Information Technology*, vol.37, no.2, pp 161-178

108. O'Malley, K.J., Cook, K.F., Price, M.D., Wildes, K.R., Hurdle, J.F., and Ashton, C.M. (2005) "Measuring Diagnoses: ICD Code Accuracy," *Health Services Research*, vol.40, no.5, part II, pp 1620-1639

109. Peyton, L., Hu, J., Doshi, C., and Seguin, P. (2007) "Addressing Privacy in a Federated Identity Management Network for E-Health", *World Congress on the Management of eBusiness*

110. Poon, E.G., Cina, J.L., Churchill, W., Patel, N., Featherstone, E., Rothschild, J.M., Keohane, C.A., Whittermore, A.D., Bates, D.W., Gandhi, T.K., (2006) "Medication Dispensing Errors and Potential Adverse Drug Events before and after Implementing Bar Code Technology in the Pharmacy" *Annals of Internal Medicine*, vol. 145, pp 426-434

111. Psaty, B.M., Boineau, R., Kuller, L.H., Luepker, R.V. (1999) "The Potential Costs of Upcoding for Heart Failure in the United States," *The American Journal of Cardiology*, vol. 84, pp. 108–109

112. Pondexter, J.C, Earp, J.B., Baumer, D.L. (2006) "An Experimental Economics Approach Toward Quantifying Online Privacy Choices," *Information Systems Frontier*, vol. 8, pp 363-374

113. Pumphrey,L.D., Trimmer, K., and Beachboard, J. (2007) "Enterprise Resource Planning Systems and HIPAA Compliance," *Research in Healthcare Financial Management*, vol. 11, no. 10, pp 57-75

114. Raghupathi, W., Kesh, S. (2007) "Interoperable Electronic Health Records Design: Towards a Service-oriented Architecture," *e-Service Journal*, pp. 39-57

115. Raman, A. (2007) "Enforcing Privacy through Security in Remote Patient Monitoring Ecosystems," *6th International Special Topic Conference on Information Technology Applications in Biomedicine*

116. Ramsaroop P., Ball M.J. (2000) "A Model for More Useful Patient Health Records," *MD Computing*, vol.17, no.4, pp 45-48

117. Reidl, B., Neubauer, T., Goluch, G., Boehm, O., Reinauer, G., and Krumboeck, A. (2007) "A Secure Architecture for the Pseudonymization of Medical Data," *Proceedings of 2nd International Conference on Availability, Reliability and Security*

118. Reiss, S. P. (1984) "Practical Data-Swapping: The First Steps," *ACM Transactions on Database Systems*, vol.9, no.1, pp 20-37

119. Rindfleisch, T.C. (1997) "Privacy, Information Technology, and Health Care," *Communications of the ACM*,, vol.40, no.8, pp 93 – 100

120. Rosenberg, M. (2001) "A Statistical Method for Monitoring a Change in the Rate of Non Acceptable Inpatient Claims," *North American Actuarial Journal*

121. Rosenberg, M.A. (2001a) "A Decision-Theoretic Method for Assessing a Change in the Rate of Non-Acceptable Inpatient Claims," *Health Services & Outcomes Research Methodology*, vol.2, no.1, pp 19-36

122. Rosenberg, M.A. (2001b) "A Statistical Method for Monitoring a Change in the Rate of Non-Acceptable Inpatient Claims," *North American Actuarial Journal*, vol.5, no.4, pp 74-83

123. Rosenberg, M.A., Andrews, R.W., Lenk, P.J. (1999) "A Hierarchical Bayesian model for Predicting the Rate of Nonacceptable In-patient Hospital Utilization," *Journal of Business & Economic Statistics*, vol.17, no.1, pp 1-8

124. Rosenberg, M.A., Fryback, D.G., Katz, D.A. (2000) "A Statistical Model to Detect DRG Upcoding," *Health Services & Outcomes Research Methodology*, vol.1, no.3-4, pp 233-252

125. Rosenberg, M.A., Griffith, J.R. (2000) "A Management Tool for Controlling the Rate of Non-Acceptable Inpatient Hospital Claims," *Inquiry - Blue Cross and Blue Shield Association*, vol.36, no.4, pp 461-470

126. Røstad, L., and Edsburg, O. (2006) "A Study of Access Control Requirements for Healthcare Systems based on Audit Trails from Access Logs," *Computer Security Applications Conference*

127. Rothstein, M.A., Talbott, M.K. (2007) "Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications," *The American Journal of Bioethics*, vol.7, no.3, pp 38-45

128. Samarati, P. (2001) "Protecting Respondents' Identities in Microdata Release," *IEEE Transactions Knowledge and Data Eng*ineering, vol.13, no.6, pp 1010–1027

129. Sandhu, R.S., Coyne, E.J., and Youman, C.E. (1996) "Role-Based Access Control Models," *IEEE Computers*, vol.29, pp 38–47

130. Sankar, P., Moran, S., Merz, J.F., Jones, N.L. (2003) "Patient Perspectives on Medical Confidentiality: A Review of the Literature," *Journal of General Internal Medicine, vol.*18, pp 659 – 669

131. Schwartmann, D. (2004) "An Attributable Role Based Access Control for Healthcare," in Bubak, M., (Eds.) *Proceedings of International Conference on Computational Science*, pp 1148 – 1155

132. Shen, J.J., Samson, L.F., Washington, E.L., Johnson, P., Edwards, C., Malone, A. (2006) "Barriers of HIPAA Regulation to Implementation of Health Services Research," *Journal of Medical Systems*, vol.30, no.1, pp 65

133. Sijs, H.V.D., Aarts, J., Vulto, A., Berg, M. (2006) "Overriding of Drug Safety Alerts in Computerized Physician Order Entry," *Journal of Medical Informatics Association*, vol.13, pp 138-147

134. Silverman, E., Skinner, J. (2004) "Medicare Upcoding and Hospital Ownership," *Journal of Health Economics*, vol.23, pp 369-389

135. Solomon, M.R. (2007) "Regional Health Information Organizations: A Vehicle for Transforming Healthcare Delivery," *Journal of Medical Systems*, vol.31, pp 37-47

136. Sparrow, M.K. (1998) "Fraud Control in the Health Care Industry: Assessing the State of the Art," National Institute of Justice: Research in Brief

137. Sparrow, M.K. (1996) "Health Care Fraud Conrol Understanding the Challenge," *Journal of Insurance, Medicine*, vol.28, no.2, pp 86-96

138. Straub, D.W.J., and Collins, R.W. (1990) "Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy," *MIS Quarterly*, vol.14, no.2, pp. 143-156

139. Straub, D.W.J., and Welke, R.J. (1998) "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, vol.22, no.4, pp 441-469

140. Susilo, W., and Win, K.T. (2007) "Security and Access of Health Research Data," *Journal of Medical Systems*, vol.31, pp 103 – 107

141. Swedlow, A., Johnson, G., Smithline, N., Milstein, A. (1992) "Increased Costs and Rates of Use in the California Workers' Compensation System as a Result of Self-Referral by Physicians," *New England Journal of Medicine, vol.*327, no.21, 1502–1506

142. Tentori, M., Favela, J., and Rodríguez, M.D. (2006) "Privacy-Aware Autonomous Agents for Pervasive Healthcare," *IEEE Intelligent Systems*, vol.21, no.6, pp 55 – 62

143. Terry, N.P., Francis, L.P. (2007) "Ensuring the Privacy and Confidentiality of Electronic Health Records," *University of Illinois Law Review*, pp 681-735

144. Truta, T.M., and Vinay, B. (2006) "Privacy Protection: p –Sensitive k-Anonymity Property," *Proceedings of 22nd International Conference on Data Engineering Workshop*

145. Truta, T.M., Fotouhi, F., Barth-Jones, D. (2004b) "Assessing Global Disclosure Risk in Masked Microdata," *Workshop on Privacy in Electronic Society*

146. Truta, T.M., Fotouhi, F., Barth-Jones, D. (2003a) "Disclosure Risk Measures for Microdata," *International Conference on Scientific and Statistical Database Management*

147. Truta, T.M., Fotouhi, F., Barth-Jones, D. (2003b) "Privacy and Confidentiality Management for the Microaggregation Disclosure Control Method: Disclosure Risk and Information Loss Measures," Workshop on Privacy in Electronic Society

148. Truta, T.M., Fotouhi, F., Barth-Jones, D. (2004a) "Disclosure Risk Measures for the Sampling Disclosure Control Method," *ACM Symposium on Applied Computing*

149. Tsumoto, S., Yokoyama, S., and Matsuoka, K. (2007) "Mining Risk Information in Hospital Information Systems as Risk Mining," *International Conference on Complex Medical Engineering*

150. Turner, G. (2002) "HIPAA and the Criminalization of American Medicine," *Cato Journal*, vol.22, no.1, pp 121-150

151. Tyler, J.L. (2001) "The Healthcare Information Technology Context: A Framework for Viewing Legal Aspects of Telemedicine and Teleradiology," *Hawaii International Conference on System Sciences*

152. US Congress (2007a) "Health Information Privacy and Security Act," S.1814

153. US Congress (2007b) "National Health Information Technology and Privacy Advancement Act of 2007," S.1455,

154. US Congress (2008) "Technologies for Restoring User's Security and Trust in health Information Act of 2008," H.R.5442

155. Vaast, E.(2007) "Danger is in the Eye of the Beholders: Social Representations of Information Systems Security in Healthcare," *Journal of Strategic Information systems*, vol.16, pp 130-152

156. Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W., Middleton, B. (2005) "The Value of Health Care Information Exchange and Interoperability," *Health Affairs*

157. Wall Street Journal (2008) "Are Your Medical Records at Risk?" April 29

158. Walsh, K.E., Adams, W.G., Bacuhner, H., Vinci, R.J., Chessare, J.B., Cooper, M.R., Hebert, P.M., Schainker, E.G., and Landrigan, C.P. (2006) "Medication Errors Related to Computerized Order Entry for Children," *Pediatrics*, vol.118, no.5, pp 1872-1879

159. Warkentin, M., Johnson, A.C., Adams, A.C., (2006) "User Interaction with Healthcare Information Systems: Do Healthcare Professionals Want to Comply with HIPAA?" *American Conference of Information Systems*

160. Win, K.T., Susilo, W., and Mu, Y. (2006) "Personal Health Record Systems and Their Privacy Protection," *Journal of Medical Systems*, vol.30, pp 309 – 315

161. Winkler, W.E.(2004) "Masking and Re-identification Methods for Public-Use Microdata: Overview and Research Problems," in *Privacy in Statistical Databases*, J. Domingo-Ferrer and V. Torra (Eds.), pp. 231–246

162. Xu,S.(2007) "Advancing Return on Investment Analysis for Electronic Health Record Investment: Impact of Payment Mechanisms and Public Returns," *Journal of Health Information Management*, vol.21, no.4, pp. 32-39

163. Zhao, X., and Johnson, M.E. (2008) "Information Governance: Flexibility and Control through Escalation and Incentives," *Workshop on the Economics of Information Security*, Hanover, NH

164. Zheng, Y., Chen, Y., Hung,, P.C.K. (2007) "Privacy Access Control Model with Location Constraints for XML Services," *International Conference on Data Engineering Workshop*

Appendix 1: Classification of Research in Healthcare Information Security and Privacy

* Categories: **Qualitative Research:** (1) Policy Report, (2) Topical Discussion, (3) Literature Survey, (4) Case Study, (5) Theory Building, (6) Interview; **Quantitative Research:** (7) Empirical study with primary data, (8) Empirical study with secondary data, (9) Economic Modeling, (10) Mathematical/ Statistical Modeling; **Design Research:** (11) Algorithm ,(12) Architecture/ Framework, (13) Measurement, (14) Experimental /Simulation, (15) Conceptual Modeling, and (16) Prototyping.

Articles / Categories*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Information Access Control																
Al-Nayadi, Abawjy (2007)												X				
Ball et al. (2003)															X	X
Bhatti, Grandison (2007)											X	X				
Chen, et al. (2005)												X				
Covington, et al. (20000												X				
Ferreira et al. (2006)												X				
Li, Tripunitara (2006)										X	X	X				
Malin, Arioldi (2007)												X			X	
Motta, Furuie (2003)										X		X				X
Nepal et al. (2006)												X				X
O'Kefee et al. (2005)												X				X
Reidl et al. (2007)												X				
Rostad, Edsberg (2006)							X									
Schwartmann (2004)												X				
Tentori et al. (2006)												X			X	X
Information Security for Authorized Data Disclosure																
Agrawal, et al. (2004)												X		X		
Agrawal, et al. (2002)		X										X				
Agrawal, Evifimievski, Kiernan, Velu										X	X			X		
Agrawal, Johnson (2007)		X										X				
Behlen, Johnson (1999)		X														
Chao, Twu, Hsu (2005)										X	X	X		X		
Domingo-Ferrer, et al. (2006)										X	X					
Domingo-Ferrer, Mateo-Sanz (2002)										X	X					
Hasan, Yurcik (2006)								X								
Hong, et al. (2007)										X		X				
Malin (2007)					X					X	X					
Muralidhar and Sarathy (2005)										X	X					
Reidl et al. (2007)												X				
Samarati (2001)										X	X					
Susilo, Win (2007)										X						
Truta, et al. (2007)					X					X	X			X		
Truta, Vinay (2006)					X					X	X					
Winkler (2004)		X	X													
Information Security on Web Enabled Care Provision																
Ball, Gold (2006)			X	X												
Cheng, Hung (2006)													X			
Choudhury, Ray (2007)													X			
Dong, Dulay (2006)													X			
Gallaher, et al. (2002) : NIST Report	X			X			X									
Gold, Ball (2007)													X			
Hu, Ferraiolo, Kuhn (2006): NIST	X	X											X			
Hung (2004)												X				

Articles / Categories*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Peyton, Hu, Doshi, Seguin (2007)				X								X				
Ramsaroop, Ball (2000)																
Yasnoff (2005)																
Zheng et al. (2007)			X									X				
Information Integrity in Healthcare and Adverse Effects																
Aarts et al. (2004)				X	X											
Applebaum (2002)		X	X													
Han et al. (2005)							X									
Koppel et al. (2005)							X									
Poon et al. (2006)							X									X
Sijs et al. (2006)			X													
Upperman et al. (2005)							X									
Walsh et al. (2006)				X			X									
Privacy Concerns among Healthcare Consumers																
Angst, Agarwal, Downing (2006)					X		X									
Bansal et al. (2007)					X		X									
Campbell et al. (2007)				X			X									
Sankar et al. (2003)			X													
Regulatory Compliance																
Davidson, Chismar (2007)					X		X									
Inquilla, et al. (2007)							X									
Kaiser (2004)		X														
Kaiser (2006)		X														
Miller, Tucker (2007)					X			X								
Ness (2007)							X									
Warkentin et al. (2006)					X		X									
Information Security Risk Management																
Alberts, Dorofee (2003)										X		X				
Aven, Eidsen (2007)										X						
Domingo-Ferrer et al. (2001)										X						
Lambrinoudakis et al. (2005)										X						
Maglogiannis, Zafiropoulos (2006)										X		X				
Truta et al. (2004a)					X					X		X	X	X		
Truta et al. (2004b)					X					X		X	X	X		
Truta, et al. (2003a)										X		X	X	X		
Truta, et al. (2003b)										X		X	X	X		
Winkler (2004)					X								X			
Financial Risk and Fraud Control																
Becker, et al. (2005)								X								
CMS (2008)	X						X									
FBI (2007)	X						X									
FORE (2005)	X						X									
Lorence, et al. (2002a)							X	X								
Lorence, et al. (2002b)							X	X								
Lorence, Richardson (2002)							X	X								
O'Malley, et al. (2005)		X														
Psaty, et al. (1999)							X	X								
Rosenberg (1999)								X		X		X				
Rosenberg (2001a)								X		X		X				
Rosenberg (2001b)								X		X		X				
Rosenberg, et al. (2000)								X		X		X				
Rosenberg, Griffith (2000)								X		X		X				
Silverman, Skinner (2004)								X								

Articles / Categories*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Sparrow (1996)		X														
Sparrow (1998)		X														
Xu (2007)																
Regulatory Implication to Healthcare Practice																
Applebaum (2002)		X	X													
Baker (2006)		X	X													
Cate (2002)		X														
Epstein (2002)		X														
Finne (1996)		X													X	
Gostin, et al. (2001)		X										X				
Gostin, Hodge (2002)		X														
Hodge (2006)		X														
Hodge, et al. (1999)		X														
Hodge, Gostin (2006)		X														
Hyman (2002)		X						X								
Lounsbury, et al. (2007)		X														
Magnusson (2006)		X														
Mandl et al. (2001)		X														
Pumphrey, Trimmer, Beachboard (2007)		X														
Rothstein, Talbott (2007)		X						X								
Shen, et al. (2006)				X												
Solomon (2007)		X		X												
Terry, Francis (2007)		X														
Tyler (2001)		X														