Information security and privacy in healthcare: current state of research

Ajit Appari and M. Eric Johnson*

Glassmeyer/McNamee Center for Digital Strategies,
Tuck School of Business,
Dartmouth College, Hanover, NH 03755, USA
E-mail: Ajit.Appari@Tuck.Dartmouth.Edu
E-mail: M.Eric.Johnson@Tuck.Dartmouth.Edu
*Corresponding author

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

Keywords: information security; privacy; healthcare; research literature.

Reference to this paper should be made as follows: Appari, A. and Eric Johnson, M. (2010) 'Information security and privacy in healthcare: current state of research', *Int. J. Internet and Enterprise Management*, Vol. 6, No. 4, pp.279–314.

Biographical notes: Ajit Appari is a Research Fellow at Tuck's Glassmeyer/ McNamee Center for Digital Strategies, Dartmouth College. His research focuses on the managerial and policy issues associated with the use of IT in healthcare such as information security and privacy, diffusion of IT, and its value impact. His research has been published in journals including *IEEE Software*, and peer-reviewed conferences including *Workshop on Economics of Information Security*, *Workshop on Information Security and Privacy*, and *American Conference on Information Systems*. He holds a PhD in Business Administration from Syracuse University, and Master of Technology from the Indian Statistical Institute, India.

M. Eric Johnson is Director of Tuck's Glassmeyer/McNamee Center for Digital Strategies and the Benjamin Ames Kimball Professor of the Science of Administration Management at the Tuck School of Business, Dartmouth College. His teaching and research focuses on the impact of information technology on business processes. He has testified before the US Congress on information security and published many related articles in the *Wall Street Journal*, *Financial Times*, *Sloan Management Review*, *Harvard Business Review*, and *CIO Magazine*. He holds a BS in Engineering, BS in Economics, an MS in Engineering from Penn State University, and a PhD in Engineering from Stanford University.

1 Introduction

Healthcare information systems are largely viewed as the single most important factor in improving US healthcare quality and reducing related costs. According to a recent RAND study, the USA could potentially save $81B annually by moving to a universal Electronic Health Record (EHR) system (Hillestad et al., 2005). Not surprisingly, recent government initiatives have pushed for wide-scale adoption of universal EHR by 2014 (Goldschmidt, 2005). Yet, IT spending in healthcare sector trails that of many other industries, typically 3–5% of revenue, far behind industries like financial services where closer to 10% is the norm (Bartels, 2006). Anecdotal evidences from recent years suggest that a lack of adequate security measures has resulted in numerous data breaches, leaving patients exposed to economic threats, mental anguish and possible social stigma (Health Privacy Project, 2007). A recent survey in the USA suggests that 75% of patients are concerned about health websites sharing information without their permission (Raman, 2007). Possibly, this patient perception is fuelled by the fact that medical data disclosures are the second highest reported breach (Hasan and Yurcik, 2006). In response to these increasing threats to health information and privacy, new regulations at both the state and the federal level have been proposed in the USA, e.g., Health Insurance Portability and Accountability Act (HIPAA).

Over the past two decades, information security research has become a well-established area within the information systems discipline. Researchers have adopted several underlying theories from reference disciplines such as psychology and sociology to analyse information security risk management (Baker et al., 2007; Dhillon and Backhouse, 2001; Straub and Collins, 1990; Straub and Welke, 1998; Vaast, 2007) and economic theories to characterise investment decisions and information governance (Cavusoglu et al., 2004, 2005; Gordon and Loeb, 2002; Khansa and Liginlal, 2009; Kumar et al., 2007; Zhao and Johnson, 2008). Despite this growing stream of research on information security, very limited research has focused on studying information security risks in the healthcare sector, which is heavily regulated and calls upon business models different from other industries.

Since Anderson's seminal work on security in healthcare information systems (Anderson, 2004), scholars have examined information security issues from many different perspectives. In this paper, we review the current state of information security and privacy research in healthcare, covering various research methodologies such as design research, qualitative research and quantitative research. Our review illuminates the multifaceted research streams, each focusing on special dimensions of information security and privacy. For example, on the one hand, a large body of research focuses on developing technological solutions for ensuring privacy of patients while their information is stored, processed and shared. On the other hand, several researchers have examined the impact of health IT adoption on care quality. Additionally, the enactment of the HIPAA and emergence of web-based healthcare applications have turned researchers' attention towards patient as well provider perspectives on HIPAA. Surprisingly, very limited attention has been given to the economics of information security risks (e.g., financial risks arising from medical identity theft and healthcare fraud).

In this paper, first we present a general view of information flow in healthcare and the evolving regulatory landscape. Next, we identify several research domains that we use to classify the literature. Building on this classification, we summarise 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 viewed as a key governing principle of the patient–physician relationship. Patients are required to share information with their physicians to facilitate correct diagnosis and treatment, and to avoid adverse drug interactions. However, patients may refuse to divulge important information in cases of health problems such as psychiatric behaviour and HIV, as their disclosure may lead to social stigma and discrimination (Applebaum, 2002). Over time, a patient's medical record accumulates significant personal information including identification, history of medical diagnosis, digital renderings of medical images, treatments, medication history, dietary habits, sexual preference, genetic information, psychological profiles, employment history, income and physicians' subjective assessments of personality and mental state (Mercuri, 2004).

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

Figure 1 **A graphical view of information flow in the health care system (see online version for colours)** Org5nvu

In the last four decades, the US healthcare industry has undergone revolutionary changes, driven by advances in IT and legislation such as the Health Maintenance Organizations Act of 1973, the landmark Health Insurance Portability and Accountability Act (HIPAA) of 1996, and national initiatives such as 'State Alliance for eHealth' started in 2007 by National Governors Association Centre for Best Practices. The Privacy and Security Rule of HIPAA requires covered entities to ensure implementation of administrative safeguards in the form of policies, personnel and physical safeguards to their information infrastructure, and technical safeguards to monitor and control intra and inter-organisational information access (Choi et al., 2006). As personal health information is digitised, transmitted and mined for effective care provision, new threats to patients' privacy are becoming evident (Mercuri, 2004). In view of these emerging threats and the overarching goal of providing cost-effective healthcare services to all citizens, several important federal regulations are being considered by the US Congress, including the Health Information Privacy and Security Act, National Health IT and Privacy Advancement Act of 2007, and Technologies for Restoring Users' Security and Trust in Health Information Act of 2008 (USC, 2007a, 2007b; 2008). In addition, nearly 60 Health-IT-related laws have been enacted in 34 states, plus the District of Columbia (RTI, 2007). The intent of this body of legislation is to improve the privacy protection offered under existing regulations by: creating incentives to de-identify health information, establishing health IT and privacy systems, bringing equity to healthcare provision and increasing private enterprise participation in patient privacy.

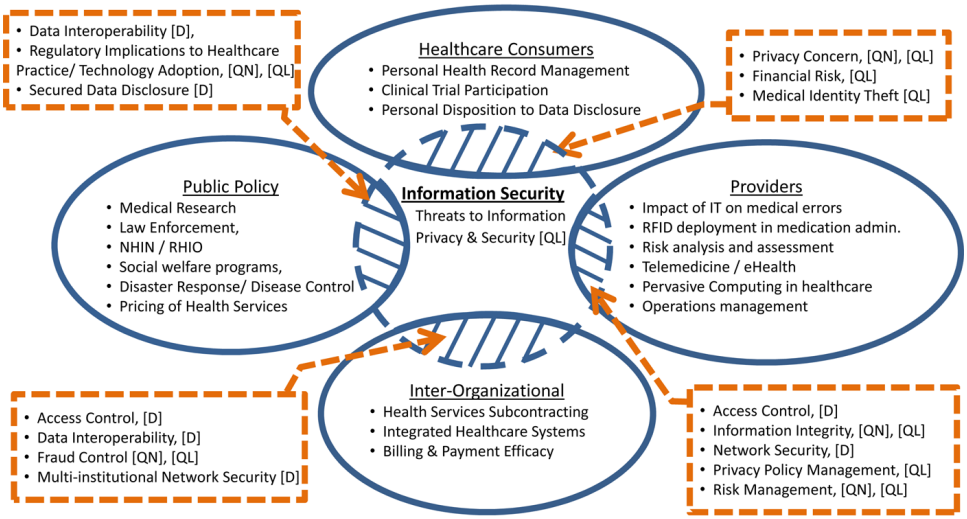
3 State of information security research in healthcare

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

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

healthcare technology adoption and secured data disclosure mechanisms) have emerged in the public policy domain, particularly in areas such as medical research, development of national health information network, disaster response and pricing of health services.

Figure 2 Research domains in the healthcare information security (see online version for colours)



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

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

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

3.1 Threats to information privacy

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

1 organisational threats that arise from inappropriate access of patient data by either internal agents abusing their privileges or external agents exploiting a vulnerability of the information systems

2 systemic threats that arise from an agent in the information flow chain exploiting the disclosed data beyond its intended use (NRC, 1997).

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

- *Accidental disclosure*: Healthcare personnel unintentionally disclose patient information to others (e.g., e-mail message sent to wrong address or inadvertent web-posting of sensitive data).
- *Insider curiosity*: An insider with data-access privilege pries upon a patient's records out of curiosity or for their own purpose (e.g., a nurse accessing information about a fellow employee to determine possibility of a sexually transmitted disease or medical personnel accessing potentially embarrassing health information about a celebrity and transmitting it to the media).
- *Data breach by insider*: Insiders access patient information and transmit it to outsiders for profit or revenge.
- *Data breach by outsider with physical intrusion*: An outsider enters the physical facility either by coercion or forced entry and gains access to the system.

- *Unauthorised intrusion of network system*: An outsider, including former employees, patients, or hackers, intrudes into an organisation's network from the outside to gain access to patient information or render the system inoperable.

Systemic Threats: Etzioni (1999), in discussing the 'limits to privacy', observed that a major threat to patient privacy occurs, not from outside of the information flow chain, 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 terminate employment. Patients or payer organisations may incur financial losses from fraud including upcoding of diagnoses or for rendering medically unnecessary services.

3.2 Privacy concern among healthcare consumers

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

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

Bansal et al. (2007) 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 websites. In particular, they reported that users' current health status, personality traits, culture, and prior experience with websites and online privacy invasions play a major role in users' trust in the health website and their degree of privacy concerns. On the other hand, in a mail-based survey with adult patients in England, Campbell et al. (2007) found that about 28–35% 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 used their health information for a wide variety of purposes, including combining data with other patients' data to provide better information to future patients, sharing treatment outcomes with other physicians, teaching medical professionals and writing research articles about diseases and treatments.

In another study, Angst et al. (2006) investigated the divergence of perception among patients towards different types of personal health record systems (in an increasing order of technological advancement), including paper-based, personal-computer-based, memory devices, portal and networked PHR. The study found that patients' 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. However, technologically advanced PHR systems were found to be favoured by highly educated patients.

3.3 Providers' perspective of regulatory compliance

HIPAA compliance has become a business necessity in Healthcare Maintenance Organisations (HMOs). Recently, Warkentin et al. (2006) undertook a study to characterise the compliance behaviour 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 with 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 behavioural intent of healthcare professionals, including medical and administrative staff, was positively correlated to self-efficacy and perceived organisational support. Another set of studies showed that healthcare workers were highly concerned about maintaining accuracy of patient records and about unauthorised access to patient data. They also believed that patient data should not be used for unrelated purposes except for medical research (Baumer et al., 2000).

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

An adverse view of HIPAA is also reflected in lower adoption rates of health information systems such as EMR bolstering the perception that privacy laws may actually have a negative effect on the ulterior goals of providing quality care at low cost. Recently, Miller and Tucker (2009) examined data on enactment of state privacy laws regulating health information disclosure across the USA and the adoption rate of EMR. They found that hospitals in states with privacy laws were 24% less likely to adopt an EMR system. However, in states with no privacy laws, they found that a hospital's adoption of EMR increases the likelihood of neighbouring hospital adopting EMR by about 7%. Without other incentives, this adverse effect may hinder the goal of establishing an interoperable national health network.

The quality of administrative capabilities in managing access control 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 are often considered one of the major software applications that could streamline business processes (Jenkins and Christenson, 2001). This is especially true if patient health data could be combined with financial information, eliminating the need for redundant data entry and facilitating clinical decision-making. However, many ERP systems require customisation to ensure HIPAA compliance. Pumphrey et al. (2007) recommend that organisations establish comprehensive policies for privacy and security management and ensure that technology vendors address these policies in the software.

3.4 Information-access control

Modern healthcare systems are large networked systems managing patient data with a multitude of users accessing health data for diverse contextual purposes within and across organisational boundaries. Role-Based Access Control (RBAC), originally developed to manage access to resources in a large computer network (Ferraiolo and Kuhn, 1992; Sandhu et al., 1996), is generally presented as an effective tool to manage data access because of its ability to implement and manage a wide range of access control policies based on complex role hierarchies commonly found in healthcare organisations (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 theorised to reduce the burden of managing access privileges by lowering the number of permissions and roles to a manageable size and hence reducing administrative cost. In addition, progress is being made in several fronts, including the use of autonomous agents to create privacy-aware healthcare applications (Tentori et al., 2006), authorisation policy framework for peer-to-peer distributed healthcare systems (Al-Nayadi and Abawajy, 2007), encrypted bar code frameworks for electronic transfer of prescription (Ball et al., 2003), pseudonymous linkage (Reidl et al., 2007) and electronic consent models that allow patients to define which component of a medical record can be shared and with whom (O'Keefe et al., 2005; Nepal et al., 2006).

Despite significant progress in technological solutions to information-access control, operationalisation remains a major challenge (Lovis et al., 2007). Healthcare organisations, because of the complex nature of data access for diverse purposes, often give broader access privileges and adopt 'Break the Glass' (BTG) policies 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. They also found that security mechanisms of health information systems were overridden to access 54% of patients' records. A common pitfall of BTG policy is that such broad-based privileges can be misused by employees. To address these issues, Bhatti and Grandison (2007) proposed a privacy management architecture (PRIMA) that leverages artefacts 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 (outside of the patients' consent). In a related study, Malin and Airoldi (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.

In summary, a significant body of research has been developed in the domain of information-access control offering technological solutions to manage data-access privileges in healthcare organisations. Yet, access control management is not just a technical solution but requires consideration of work processes, organisational structure and culture to provide effective information security (e.g., Ferreira et al., 2006). The effectiveness of an access control system depends on how the users interact with the system and the incentives to treat data properly (Zhao and Johnson, 2008). To improve the transparency of access control management, some hospital systems have even adopted the policy of sharing audit logs with patients, thus enabling them to continually refine access rights on their own health records (Lovis et al., 2007).

3.5 Data interoperability and information security

Many healthcare information systems currently in use store information in different proprietary formats. This diversity of data formats creates a major hurdle in sharing patient data among provider organisations, not to mention data for research. In a recent investigation, Walker et al. (2005) empirically argued that investing in EMR interoperability and establishing a health information exchange could save the industry $77B annually. 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 one of the 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

(AHRQ 2007a). While most of these state plans recognise the need and call for development of a universal patient consent form that incorporates common information disclosure situations as well for specially protected information, a significant focus has been given to the development of standardised approaches for user authorisation, authentication, access, uniform identification of patients, audit of health record access and modification logs, and security of data during transmission (AHRQ 2007b).

Development of a fully functional interoperable EHR system remains a major challenge. Recent research has proposed prototypes of Service-Oriented Architecture (SOA) models for EHR in various contexts including clinical decision support (Catley et al., 2004), collaborative medical (mammogram) image analysis (Estrella et al., 2004) and health clinic settings (Raghupathi and Kesh, 2007). These SOA-based EHRs are expected to be scalable to enable inter-enterprise environments, such as RHIO, and alliances of such RHIOs could lead to national and global health information networks (Raghupathi and Kesh, 2007). Using a case study analysis of three emerging RHIOs (namely the Indian health Information Exchange, the Massachusetts Health Data Consortium and the Santa Barbara County Care Data Exchange), Solomon (2007) elicited several factors that influence innovation and diffusion, adaptation and change management of RHIOs. Among them, privacy and security of patient information are major concerns hampering the adoption of clinical information technologies across the RHIOs and consumers. Such concerns could remain in the near future, as the technology standards for data interoperability are still in the development stage (Dogac et al., 2006; Eichelberg et al., 2005). Moreover, Solomon point out that in order for RHIOs to become a major agent of transformation, effective regulations are required to strengthen the protection of PHI by devising comprehensive privacy and security standards that allow RHIOs to avoid the traps of state-specific regulations.

3.6 Information security issues of e-health

The emergence of internet technologies has transformed the business model for customer-oriented industries such as retail and the financial services. The healthcare sector is also experiencing a tectonic shift in enablement of healthcare services through internet and mobile technologies such as remote health monitoring, online consultation, e-prescription, e-clinical trials, patient information access and asset tracking among others (Kalorama Information, 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 a health bank, first conceptualised 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 Microsoft's 'Health Vault' and 'Google Health' are examples of such health banking systems. However, such web-enabled and mobile-based services open up a whole gamut of security risks compounding the privacy problem. A growing body of research is focused on developing mechanisms to address privacy and security concerns related to internet and mobile healthcare applications (e.g., Dong and Dulay, 2006; Hung, 2005; Peyton et al., 2007; Raman, 2007; Zheng et al., 2007). For example, the development of a 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 a patient's location. Thus, to ensure integrity and confidentiality of patient data, direct downloading of a patient's record to a PDA owned by a healthcare professional visiting the patient must be constrained by location or ownership information (Zheng et al., 2007). Advances have been made to incorporate device location or ownership constraints to strengthen the privacy-enabled RBAC system (Hung, 2005; Cheng and Hung, 2005). In another study, Chowdhury and Ray (2007) present a 'cooperative management' methodology for assuring privacy of different stakeholders interacting via web-based applications.

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

1 a privacy officer or regulatory agency to validate privacy compliance or investigate allegations of privacy breaches

2 individual patients to verify how their data is being used and challenge data accuracy.

From the public policy perspective, recent research indicates that the promulgation of HIPAA has created greater transparency among the healthcare institutions such as insurance and pharmacies, yet their privacy policies are often more difficult to comprehend (Anton et al., 2007).

3.7 Information security risks in authorised data disclosure

In the healthcare sector, it is often necessary to share data across organisational boundaries to support the larger interests of multiple stakeholders as well as agencies involved with public health. However, the release of patient data could entail personally identifying information as well sensitive information that may violate privacy as well cause socio-economic repercussions for patients. Yet such data, when masked for identifying and sensitive information, must maintain the analytic properties to assure statistical inferences, especially when released for epidemiological research (Truta et al., 2004a, 2004b). Advances in technology have enabled the consolidation of health records from multiple sources to a single research database, which supports researchers engaged in public health, clinical methods and health services in general.

A growing body of research, building on the theory of statistical disclosure control, offers a diverse range of data-masking methodologies and frameworks to minimise or control the disclosure risk of patient information (e.g., global and local recoding (Samarati, 2001), microaggregation (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, 2005), 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, which require identification of the patient for corrective follow-up care. Additionally, links are needed to control research validity (prevent frauds) and reduce the 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 using the *k*-anonymity algorithm (Truta and Vinay, 2006) to maintain confidentiality of patients during data disclosure. Similarly, set theory can be 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 a patient and his/her health record that would allow authorisation to approved individuals, including healthcare providers, relatives and researchers.

Theoretical advances in data masking, discussed earlier, are also being strengthened contemporaneously with industrial research and technological advances such as the Hippocratic database (Agrawal et al., 2002) and the Sovereign Information Sharing platform (Agrawal et al., 2003, 2004). The 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 the acquisition of privacy preferences from patients under the aegis of e-health applications built on the 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).

Data dissemination for purposes other than care provision presents many challenges. In protecting 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. An emergent body of research focusing on the development of data disclosure methods, and evaluation of such methods, employs a variety of measures for disclosure risk and information loss (e.g., Truta et al., 2003a, 2003b, 2004a, 2004b; Winkler, 2004). For example, Truta et al. (2003a) define 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 data are extricated in the released data set

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 assumptions about the extent of prior knowledge an intruder may have from external sources. In another study, Truta et al. (2004a) considered a data-sampling method to assess its performance with respect to the above-mentioned three risk measures. More recently, Truta and his colleagues extended this line of research by considering new dimensions in data disclosure – the potential utility for intruders and the ordered relation of attributes that could be exploited by intruders (e.g., 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 minimise information. The measurement of information loss, however, depends on potential usages of released data, which is difficult to anticipate at the time of disclosure (Domingo-Ferrer and Torra, 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 and Torra (2001) taking into account the peculiarity of health data. More recently, El Emam and his colleagues extend this research stream by comparative evaluation of some of the most commonly used de-identification heuristics for disclosure of patient information for public health and health services research, development of new heuristics for such disclosures that ensure balanced trade-off between disclosure risk and information loss, and estimation of population size cut-off at which data suppression could prove fruitful strategy for data disclosure (El Emam, 2008; El Emam and Dankar, 2008; El Emam et al., 2006, 2007, 2009).

3.8 Information integrity in healthcare and adverse effects

Information security risks are often described by terms like ‘data breach’, ‘hackers attack’ and ‘data theft’ in the mainstream media. However, one of the key concepts of information security is ensuring data integrity in addition to confidentiality and availability. In the healthcare sector, faulty system design features could become a primary internal threat to information security. For example, the integrity of medical records may be compromised by poor alert design. Recent research has shown that excessive alerts may cause ‘alert fatigue’ leading clinicians to override alerts, and ultimately impacting patient safety (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 papers related to Computerised Physician Order Entry (CPOE) systems and Clinical Decision Support Systems (CDSS) using *Reason’s framework of accident causation* and concluded 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 the prevalence of larger patient data repositories across US hospitals for medical decision-making, giving rise to concerns on quality and reliability of patient data for effective medical decision-making (Lorence et al., 2002a, 2002b). In a survey of health information managers, Lorence (2003) discovered that, despite a national mandate to promote and adopt uniform data quality management, about 39% of health information managers indicated that their organisations 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

2 errors arising from the human–machine interfaces that do not reflect conventional behaviour and the 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 paediatric support. Many of these concerns stem from the lack of integration of CPOE with other systems like inventory control systems (Inquilla et al., 2007) or poor design and policy features of the systems (Aarts et al., 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.

3.9 Financial risk and fraud control

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

Healthcare providers throughout the US document diagnosis using the International Classification of Diseases (ICD), which has over 120,000 codes (O'Malley et al., 2005). In addition to classifying morbidity and mortality information, the coding system serves various purposes including reimbursement, administration, epidemiology and health services research. For billing purposes, ICD codes are grouped at a macrolevel according to Drug-Related Group (DRG) coding principles. O'Malley et al. (2005) note that as patients proceed through the process of arrival to discharge, the documentation errors can creep into patients' medical records from different sources. For example, data errors

can result from the amount and quality of information being gathered at admission, communication quality between patients and clinicians, clinical training and experience, transcription error, training and experience of coders, and incorrect bundling of codes (O'Malley et al., 2005). In a recent survey of information managers, Lorence et al. (2002a, 2002b) reported that about 14% of managers agreed 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).

Information security risks in healthcare have monetary consequences to multiple stakeholders including patients, healthcare organisations 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, the General Accounting Office of USA 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). Federal initiatives have taken aim at these losses, including the *healthcare fraud and abuse programme* (as part of the HIPAA). Since then, fraud control units at Center for Medicare and Medicaid Services (CMS) investigate submitted claims and compare them with patients' medical record to identify occurrence of fraud and prosecute the fraudulent entities. A series of audit-based studies have been conducted in the past to identify determinants of healthcare fraud, in particular the observable characteristics of providers and claims associated with fraudulent behaviour (Hillman et al., 1990; Psaty et al., 1999; Silverman and Skinner, 2004; Swedlow et al., 1992). Silverman and Skinner (2004) found evidence that upcoding behaviour (i.e., the practice of billing for higher charges) at non-profit hospitals is similar to that of for-profit hospitals. More recently, an empirical study by Becker et al. (2005) concluded that increased expenditures at the Medicare Fraud Control Unit (MFCU) reduced upcoding.

In a detailed investigation of why fraud plagues the US healthcare system, Sparrow (1996, 1998) argued that fraud control is a very complex endeavour and that most insurers have failed to measure the magnitude of the problem. Currently, organisations use various approaches including automated claims auditing, manual examination or audits of submitted claims, pre-payment medical review and post-payment utilisation review (Sparrow, 1998). Among them, they found that post-payment utilisation review is the major tool used by payer organisations. Using that tool, sampled medical records associated with episodes of inpatient claims are audited to detect fraudulent behaviour of healthcare providers – an expensive undertaking for payer organisations (Rosenberg, 2001a, 2001b). A growing body of research has focused exclusively on the usage of readily available data from the Universal Billing Form (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, 2001a, 2001b; Rosenberg et al., 1999, 2001; Rosenberg and Griffith, 2000). 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 a sample, 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 (DRGs) using a Bayesian logistic regression model on the audited claims, 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 an *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). The approach makes use of decision rules in the sense that if the expected loss is lower than the expected audit cost, the statistical monitoring model recommends no investigation for the principal diagnosis under review. Payer organisations equipped with such statistical monitoring tools for controlling the NAC rate could direct their resources to other necessary services rather than on expensive audits (Rosenberg, 2001b).

3.10 Regulatory implications to healthcare practice

A significant body of public policy research, both in medical informatics and in law, also investigates the implications of privacy and security. Much of this work has focused on the legal aspects of EHR and privacy facilitation through technology and policies (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); tradeoffs between personal privacy and population safety (Baker, 2006; Gostin et al., 2001; Gostin and Hodge, 2002; Hodge, 2006; Hodge and Gostin, 2004).

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., Kremer 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 and Talbott (2007) present an 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 and automobile insurance claims), Rothstein and Talbott (2007) projected that, on average, 25 million 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, Rothstein and Talbott (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, many have argued that concerted efforts are needed to provide privacy safeguards based on fair information practices, industry-wide protection, and an established national data protection authority (Hodge et al., 1999).

In psychosocial and health-behavioural research, medical researchers often collect information on 'third parties' who are related to research participants. Building upon recommendations by the Office for Human Research Protections (OHRP) and Botkin (2001), Lounsbury et al. (2007) propose a rule set that could be adopted by 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 authorisation. Yet, the onus of justifying access to patient information lies with the 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 maximised where they are likely to achieve the greatest public good." (Hodge and Gostin, 2004, p.676)

3.11 Information security risk management

Managing information security risks is a complex process and requires investments in organisational resources and multipronged approaches such as the OCTAVE approach that uses asset-based information security assessment (Alberts and Dorofee, 2002), Bayesian network analysis (Maglogiannis and Zafiropoulos, 2006), elicitation of user's privacy valuation using experimental economics (Poindexter et al., 2006), and information security insurance contracts (Lambrinoudakis et al., 2005). The OCTAVE approach was developed at the Software Engineering Institute (SEI) at Carnegie Mellon University and was first published for public use in 2001. The approach was developed on three core groups of principles – information security risk evaluation principles (i.e., self-direction, adaptable measures, defined process and foundation for continuous improvement process), risk management principles (i.e. forward looking view to manage uncertainty, focus on critical few assets, integrated management of information security by embedding with business strategies and goals), and organisational and cultural principles (i.e., open communication of security issues, identifying security risks at local level but analysing them with a global perspective, and using an interdisciplinary team with members from both business and technology). The OCTAVE approach is considered well suited for healthcare organisations, as it offers the flexibility to meet the customised needs of an organisation depending on its size and complexity. Recent case studies indicate successful deployment of the OCTAVE approach in managing information security risks in compliance with HIPAA (Woody, 2006). More recently, an advanced version of this approach – OCTAVE Allegro – has been introduced, which focuses on information assets exclusively and considers other assets (people, process and technology) only to facilitate effective identification of threats (Caralli et al., 2007). This revised approach is expected to be easy to use, reduce the resource burden on the organisation, and reduce training and knowledge prerequisites for participants.

With the increasing adoption of online channels, it is imperative that healthcare organisations gain adequate knowledge of consumers' privacy and security perceptions and expectations. However, quantification of consumer perception is not an easy task. Poindexter et al. (2006) demonstrated that experimental economics can be used by organisations to assess consumers' valuation of privacy and of different forms of security safeguards such as encryption and regulatory compliance. They also show that the approach can be used to understand consumers' response to technology,

especially the internet. Such experiments, when adopted on broader segments of health consumers, could elicit important metrics for policy makers and security technology creators to ensure alignment of privacy and security with consumer demands.

However, investing in technological, organisational and procedural measures will never ensure complete security. Lambrinoudakis et al. (2005) argue that organisations should also adopt insurance policies to minimise financial losses from potential security incidents. They modelled the impact of security incidents on an IT system, using a Markov process to represent the transitions from a fully operational state to non-operational state. Such models could be used to estimate the desired level of insurance coverage as well the desired quantum of security investment that an organisation should undertake.

4 Conclusions and directions for future research

In this paper, we have examined the extant body of knowledge on privacy and security in healthcare, spanning several research domains including privacy concerns among healthcare consumers and providers' perspective of regulatory compliance. Our review indicates that scholars from health informatics, legal and computer science have adopted a multitude of methodologies including design research, qualitative and quantitative research methods to examine various aspects of security and privacy in the healthcare sector. Information security has drawn significant attention among mainstream information systems scholars, yet there has been relatively little published concerning the unique security challenges found in healthcare. We believe that the increasing importance of information security and the need for managerial insights to these problems offer an exceptional opportunity for debate and cross fertilisation within the IS research community. Certainly, there is a substantial need for new ideas that could guide practitioners through this time of change within the industry.

The US healthcare delivery system has evolved over the past century from a patient–physician dyadic relationship into a complex network linking patients to multiple stakeholders. IT advances and their adoption in healthcare are more likely to improve care provision quality, reduce costs, and advance medical science. However, this evolution has increased the potential for information security risks and privacy violations. Healthcare researchers can help by conducting multidisciplinary research in the domains identified in this survey to inform both theory and practice. In a recent examination of the impact of HIPAA on the integrity of healthcare information, Fedorowicz and Ray (2004) challenged the research community to conduct field studies of early adopters to assess the issues involved with HIPAA implementation, benefits of HIPAA compliance, and impact on inter-organisational relationships. A similar call for research has been suggested by Wen and Zhang (2002) to study the impact of HIPAA regulation on healthcare practice, especially in terms of technical, managerial and legal issues associated with privacy compliance promulgated by HIPAA. We echo their calls for research on HIPAA by proposing several wide-ranging topics of interest that could further enlighten information security and privacy in the healthcare sector.

Threats to Information Privacy And Security: The extant knowledge base on information security risks identifies different types of threats to privacy and security of health information. Yet, the current ad-hoc taxonomy alone may not be useful for practice.

Anecdotal evidence suggests that major threats to patient privacy are internal factors, not external (Wall Street Journal, 2008). Future research should focus on characterising these threats based on organisational contexts (e.g., providers, clinics, insurance and RHIO), which would help practitioners in developing effective information security risk monitoring and management policies. Such an effort may include identifying frequency patterns of various threats in each type of organisation as well as across the health sector. Cross-sectional and longitudinal studies of threat patterns could help in policy making as well.

Privacy concerns among healthcare consumers: With increasing reliance on web-based systems for managing health information and the deployment of personal health banks, privacy concerns of healthcare consumers have come to the forefront. Recent research in this area has often focused on restricted user bases, such as students. Future research should explore the variance of privacy preferences in the context of online systems among a broader range of users, including the general working population and senior citizens. A deeper understanding of the factors influencing healthcare consumers' willingness to disclose personal information would enable better policy making and enhance the adoption of e-health.

Providers' perspective of regulatory compliance: Regulatory mandates, such as HIPAA, are often criticised for lack of clarity. Current low levels of full compliance among hospitals call for attention from the research community to examine compliance-related issues on several fronts. For example, researchers could examine: the variance in employee security hygiene and best practices adopted by leaders to promote regulatory compliance; the effect of regulatory compliance initiatives on service quality; the economics of achieving and sustaining regulatory compliance; the issues of managing regulatory compliance across states with diverging requirements; or the effect of regulatory requirements on the digital strategies of organisations and their partners.

Information-access control: Current research on information access has primarily focused on technological solutions. There are very few economic studies that offer deeper insights on managing information-access control in a cost-effective manner. Healthcare organisations must invest in many information security measures, such as access control systems, intrusion detection systems, policies and personnel. Failure of such information security systems may disrupt business continuity and diminish operating efficiency. Provider organisations implementing mobile technologies offering ubiquitous access to patient information could realise significant benefits in terms of reduced error and increased customer satisfaction (Abraham et al., 2008). Recently, Zhao and Johnson (2008) modelled information governance using game theory to study the impact of incentives and auditing on access. Establishing and revising access control policies in hospital environments owing to the multitude of roles, interdependent information systems, and dynamic nature of role assignment is an expensive endeavour. Future field research that accounts for the peculiarities of healthcare organisations (e.g., overriding behaviour) is needed to examine healthcare's complex governance issues and to discover best practices. In our review, we find only one empirical study reporting on access privilege provision and actual usage. Furthermore, noting the complexity of process networks in healthcare, a fruitful research direction could be to develop an understanding of interdependency between business processes enabled by information systems, and how such networks could be unduly affected by information security failures.

Data interoperability and information security: The basic premise of data interoperability is to facilitate accurate and seamless data exchange within and between organisations to support timely healthcare. Recent initiatives, such as Privacy and Security Solutions to Promote Interoperable Health Information Exchange, have facilitated progress towards the formation of HIEs, enactment of state-level privacy and security legislation, and development of shared privacy and security solutions (AHRQ, 2007c). From the policy perspective, future research is needed in several areas such as the impact of legislative efforts on variations in privacy and security investments by stakeholders in the states that participate in health information exchange and the development of common data elements for consent to enable the flow of patient medical information across organisations.

Information security issues of ehealth: Over the past five years, the healthcare sector has experienced significant growth in use of mobile devices and web-based applications. Contemporaneously, information security research has focused on the development of frameworks and protocols to address security issues in e-health. In a recent examination of privacy and security issues of e-health portals, Stingl and Slamanig (2008) proposed a series of methods including pseudonymisation of metadata, multiple identities, obfuscation and anonymous authentication to counterattacks on patients' privacy especially from what could be considered as insiders (e.g., insurance companies). Future research is needed to examine the effectiveness of such privacy enhancing frameworks and protocols on operational efficiency of healthcare providers and consumer satisfaction. Another possible fertile stream of research is the study of personal health bank diffusion vis-à-vis information security risks and the impact on patients' privacy, effect on organisational security policies, and demand on information security management resources.

Information security risks in authorised data disclosure: In the past, research has focused on developing theoretical solutions for secure data disclosure. However, healthcare providers may not always deploy state-of-the-art technology to disclose data for secondary purposes. A field-level understanding of the operational effectiveness of data disclosure technology would help managers refine disclosure policies and choose appropriate data disclosure solutions.

Information integrity in healthcare: Past research examining the impact of investment in health IT on medical error has been limited to a single instantiation of system deployment. Future research is needed to span a number of CPOE installations, both at a regional and national level, to characterise the impact of such systems on information integrity and medical errors. Such studies could consider the influence of several factors such as hospital characteristics, drug safety alert overriding behaviour, false alerts due to inadequacy of knowledge base (clinical decision-support system), incomplete or erroneous patient record, and workflow interruptions or delays. Like Schmidek and Weeks (2005) who examined the correlation between adverse events and tort claims by patients of Veterans Health Administration, future studies could examine the relationship between adverse events arising from information integrity and tort claims in the general population served by HMOs.

Financial Risk: Healthcare fraud has been estimated to comprise nearly 10% of total health expenditure in USA (Dixon, 2006). Moreover, with growing digitisation of health records, medical identity theft has become a larger looming issue,

costing payers and patients. 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 organised 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 to guide information security policy development and inform health maintenance organisations as they move towards wider adoption of EHRs systems.

Regulatory implications for healthcare practice: As we highlighted earlier, there are several avenues for future research on regulatory compliance issues from the providers' perspective. However, the healthcare sector includes many other players such as payers (insurance), employers, health information exchanges, medical researchers and personal health banks. Regulations, such as HIPAA, have been promulgated to assure patients' privacy and maintain security throughout the healthcare network. From a public policy perspective, we believe that macroeconomic studies are needed to measure the effect of these regulations.

Information security risk management: Current research on information security risk management in healthcare is limited to anecdotal evidence of the successful implementation of frameworks like OCTAVE. Keeping in mind that one size does not fit all, future research should explore how such frameworks are being implemented by different organisations and examine the economics of customisation. This research could inform practitioners on best practices for implementing OCTAVE-like frameworks. Furthermore, some of the external threats that may disrupt operations require business continuity planning. Research is needed to guide healthcare organisations on continuity planning.

We trust that this review and proposed future directions will encourage further research that will offer valuable insights to decision makers in the area of healthcare information privacy and security.

Acknowledgements

This research was supported through the Institute for Security Technology Studies at Dartmouth College, under awards 60NANB6D6130 from the US Department of Commerce and US 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 US Department of Commerce, or US Department of Homeland Security.

References

Aarts, J., Doorewood, H. and 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*, Vol. 11, pp.207–216.

Abraham, C., Watson, R.T. and Boudreau, M.C. (2008) 'Ubiquitous access: on the front lines of patient care and safety', *Communications of the ACM*, Vol. 51, No. 6, pp.95–99.

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

Agrawal, R., Asonov, D., Baliga, P., Liang, L., Porst, B. and Srikant, R. (2004) 'A reusable platform for building sovereign information sharing applications', *Workshop on Database in Virtual Organizations*, Paris, France.

Agrawal, R., Evfimievski, A. and Srikant, R. (2003) 'Information sharing across private databases', *Proceedings of ACM SIGMOD*, San Diego, CA, pp.86–97.

Agrawal, R., Kiernan, J., Srikant, R. and Xu, Y. (2002) 'Hippocratic databases', *International Conference on Very Large Databases*, Hong Kong, China.

AHRQ (2007a) *Privacy and Security Solutions for Interoperable Health Information Exchange: Final Implementation Plans*, Report for Agency for Healthcare Research and Quality, and Office of national Coordinator for Health Information Technology, http://healthit.ahrq.gov

AHRQ (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, http://healthit.ahrq.gov.

AHRQ (2007c) *Privacy and Security Solutions for Interoperable Health Information Exchange: Impact Analysis*, Report for Agency for Healthcare Research and Quality, and Office of national Coordinator for Health Information Technology, http://healthit.ahrq.gov.

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

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

Anderson, R.J. (2004) *Security in Clinical Information Systems*, University of Cambridge, http://www.cl.cam.ac.uk/~rja14/Papers/policy11.pdf

Angst, C.M., Agrawal, R. and Downing, J. (2006) *An Empirical Examination of the Importance of Defining the PHR for Research and for Practice*, http://ssrn.com/abstract=904611

Anton, A.I., Earp, J.B., Vail, M.W., Jain, N., Gheen C.M. and Frink, J.M. (2007) 'HIPAA's effect on web site privacy policies', *IEEE Security & Privacy*, Vol. 5, No. 1, pp.45–52.

Applebaum, P.S. (2002) 'Privacy in psychiatric treatment: threats and response', *American Journal of Psychiatry*, Vol. 159, pp.1809–1818.

Baker, D.B. (2006) 'Privacy and security in public health: maintaining the delicate balance between personal privacy and population safety', *Proceedings of 22nd Annual Computer Security Applications Conference*, Miami, FL, pp.3–22.

Baker, W.H., Rees, L.P. and 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.

Ball, E., Chadwick, D.W. and Mundy, D. (2003) 'Patient privacy in electronic prescription transfer', *IEEE Security and Privacy*, Vol. 1, No. 2, pp.77–80.

Ball, M.J. and Gold, J. (2006) 'Banking on health: personal records and information exchange', *Journal of Healthcare Information Management*, Vol. 20, No. 2, pp.71–83.

Bansal, G., Zaheid, F.M. and Gefen, D. (2007) 'The impact of personal dispositions on privacy and trust in disclosing health information online', *Americas Conference on Information Systems*, Keystone, CO, http://aisel.aisnet.org/amcis2007/57

Bartels, A. (2006) 'US IT spending benchmarks for 2006: How to turn the CIO's bane into an effective tool for IT budgeting', *Forrester Research Report*, www.forester.com

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

Becker, D., Kessler, D. and McClellan, M. (2005) 'Detecting medicine abuse', *Journal of Health Economics*, Vol. 24, pp.189–201.

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, pp.435–443.

Bhatti, R. and Grandison, T. (2007) 'Towards improved security policy coverage in healthcare using policy refinement', in Jonker, W. and Petkovic, M. (Eds.): *Lecture Notes in Computer Sciences*, Vol. 4721, pp.158–173.

Bolin, J.N. and 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.

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.

Brailer, D.J. (2005) 'Interoperability: the key to the future health care system', *Health Affairs*, Vol. 24, No. 1, pp.W5.19–W.5.21.

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.

Caralli, R.A., Stevens, J.F., Young, L.R. and Wilson, W.R. (2007) *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, Technical Report, CMU/SEI-2007-TR-012, http://www.sei.cmu.edu/library/abstracts/reports/07tr012.cfm

Cate, F.H. (2002) 'Principles for protecting privacy', *Cato Journal*, Vol. 22, No. 1, pp.33–57.

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*, Redwood City, CA, pp.130–138.

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.

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.

Center for Medicare and Medicaid Services (CMS) (2007) *Improper Medicare Fee-for-Service Payments Report* – November 2007 Report, last accessed on 6 June, 2008 https://www.cms.hhs.gov/apps/er_report/index.asp

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.

Chao, H.M., Hsu, C.M. and 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.

Cheng, V.S.Y. and Hung, P.C.K. (2005) 'Towards an integrated privacy framework for HIPAA-compliant web services', *Proceedings of the 7th IEEE International Conference on E-Commerce Technology*, Munich, Germany, pp.480–483.

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.

Chowdhury, A. and Ray, P. (2007) 'Privacy management in consumer e-health', *Proceedings of 9th International Conference on e-Health Networking, Application and Services (HEALTHCOM)*, Taipei, Taiwan, pp.29–33.

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.

Dalenius, T. and Reiss, S.P. (1982) 'Data-swapping: a technique for disclosure control', *Journal of Statistical Planning and Inference*, Vol. 6, No. 1, pp.73–85.

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.

Dixon, P. (2006) *Medical Identity Theft: The Information Crime that Can Kill You*, The World Privacy Forum Report, http://www.patientprivacyrights.org.

Dogac, A., Namli, T., Okcan, A., Laleci, G., Kabak, Y. and Eichelberg, M. (2006) 'Key issues of technical interoperability solutions in eHealth', *Proceedings of eHealth 2006 High Level Conference Exhibition*, Spain, http://www.ehealthconference2006.org/pdf/Dogac_proc.pdf

Domingo-Ferrer, J. and Mateo-Sanz, J. (2002) 'Practical data-oriented microaggregation for statistical disclosure control', *IEEE Transactions on Knowledge and Data Engineering*, Vol. 14, No. 1, pp.189–201.

Domingo-Ferrer, J. and Torra, V. (2001) 'A quantitative comparison of disclosure control methods for microdata', in Doyle, P., Lane, J.I., Theeuwes, J.J.M. and Zayatz, L. (Eds.): *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*, Amsterdam, North-Holland, pp.111–134.

Domingo-Ferrer, J., Martinez-Balliste, A., Mateo-Sanz, J. and Sebe, F. (2006) 'Efficient multivariate data-oriented microaggregation', *The Very large Data Base Journal*, Vol. 15, pp355–369.

Dong, C. and Dulay, N. (2006) 'Privacy preserving trust negotiation for pervasive healthcare', *Proceedings of Pervasive health Conferences and Workshops*, Innsbruck, Austria, pp.1–9.

Eichelberg, M., Aden, T., Riesmeier, J., Dogac, A. and Laleci, G. (2005) 'A survey and analysis of electronic healthcare record standards', *ACM Computing Survey*, Vol. 37, No. 4, pp.277–315.

El Emam, K. (2008) 'Heuristics for de-identifying health data', *IEEE Security and Privacy*, Vol. 6, No. 4, pp.58–61.

El Emam, K. and Dankar, F.K. (2008) 'Protecting privacy using k-anonymity', *Journal of the American Medical Informatics Association*, Vol. 15, No. 5, pp.627–637.

El Emam, K., Brown, A. and AbdelMalik, P. (2009) 'Evaluating predictors of geographic area population size cutoffs to manage re-identification risk', *Journal of the American Medical Informatics Association*, Vol. 16, No. 2, pp.256–266.

El Emam, K., Jabbouri, S., Sams, S., Drouet, Y. and Power, M. (2006) 'Evaluating common de-identification heuristics for personal health information', *Journal of Medical Internet Research*, Vol. 8, No. 4, pp.e28.

El Emam, K., Neri, E. and Jonker, E. (2007) 'An evaluation of personal health information remnants in second-hand personal computer disk drives', *Journal of Medical Internet* Research, Vol. 9, No. 3, p.e24.

Epstein, R.A. (2002) 'HIPAA on privacy: its unintended and intended consequences', *Cato Journal*, Vol. 22, No.1, pp.13–31.

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, San Francisco, USA.

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

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

Fedorowicz, J. and Ray, A. (2004) 'Impact of HIPAA on the integrity of healthcare information', *International Journal of Healthcare Technology and Management*, Vol. 6, No. 2, pp.142–157.

Ferraiolo, D.F. and Kuhn, D.R. (1992) 'Role based access control', *15th National Computer Security Conference*, Baltimore, MD, pp.554–563.

Ferreira, A., Cruz-Correia, R., Antunes, L., Farinha, P., Oliveira-Palhares, E., Chadwik, D.W. and Costa-Periera, A. (2006) 'How to break access control in a controlled manner', *IEEE Symposium on Computer-Based Medical Systems*, Maribor, Slovenia, pp.847–854.

Finne, T. (1996) 'The information security chain in a company', *Computers and Security*, Vol. 15, p.297.

FORE – Foundation of Research and Education (2005) *Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities*, http://www.ahima.org/fore

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

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, http://csrc.nist.gov/groups/SNS/rbac/documents/cost_benefits/report02-1.pdf.

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.

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.

Gostin, L.O. and 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.

Gostin, L.O., Hodge, J.G. and 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.

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.

Hasan, R. and Yurcik, W. (2006) 'A statistical analysis of disclosed storage security breaches', *Proceedings of 2nd ACM Workshop on Storage Security and Survivability*, Alexandria, VA, pp.1–8.

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

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.

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.

Hillman, B.J., Joseph, C.A., Mabry, M.R., Sunshine, J.H., Kennedy, S.D. and 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, pp.1604–1608.

Hodge, J.G. (2003) 'Health information privacy and public health', *Journal of Law, Medicine and Ethics*, Vol. 31, No. 4, pp.663–671.

Hodge, J.G. (2006) 'The legal and ethical fiction of pure confidentiality', *The American Journal of Bioethics*, Vol. 6, No. 2, pp.21–22.

Hodge, J.G. and Gostin, L.O. (2004) 'Challenging themes in American health information privacy and the public's health: historical and modern assessments', *Journal of Law, Medicine and Ethics*, Vol. 32, No. 4, pp.670–679.

Hodge, J.G., Gostin, L.O. and Jacobbson, P.D. (1999) 'Legal issues concerning health information: privacy, quality, and liability', *Journal of American Medical Association*, Vol. 282, No. 15, pp1466–1471.

Hong, Y., Lu, S., Liu, Q., Wang, L. and Dssouli, R. (2007) 'A hierarchical approach to the specification of privacy preferences', *Proceedings of 4th International Conference on Innovations in Information Technology*, Dubai, pp.660–664.

Hu, V.C., Ferraiolo, D.F. and Kuhn, D.R. (2006) *Assessment of Access Control Systems*, NIST Report 7316, http://www.csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

Hung, P.C.K. (2005) 'Towards a privacy access control model for e-healthcare services', *Proceedings of 3rd Annual Conference on Privacy, Security and Trust*, New Brunswick, Canada, http://www.lib.unb.ca/Texts/PST/2005/

Hyman, D.A. (2002) 'HIPAA and health care fraud: an empirical perspective', *Cato Journal*, Vol. 22, No. 1, pp.151–178.

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.

Jenkins, E.K. and Christenson, E. (2001) 'ERP systems can streamline healthcare business functions', *Healthcare Financial Management*, Vol. 55, No. 5, pp.48–52.

Johnson, M.E. (2009) 'Data hemorrhages in the health-care sector', *Proceedings of the 13th International Conference on Financial Cryptography and Data Security*, Barbados, pp.71–89.

Kaiser, J. (2004) 'Patient records: privacy rule creates bottleneck for US biomedical researchers', *Science*, Vol. 305, No. 5681, pp.168–169.

Kaiser, J. (2006) 'Patient privacy: rule to protect records may doom long-term heart study', *Science*, Vol. 311, No. 5767, pp.1547–1548.

Kalorama Information (2007) *Wireless Opportunities in Healthcare*, www.MarketResearch.com

Khansa, L. and Liginlal, D. (2009) 'Valuing the flexibility of investing in security process innovations', *European Journal of Operational Research*, Vol. 192, No. 1, pp.216–235.

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.

Koppel, R., Metlay, J.P., 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.

Kremer, T.G. and Gesten, E.L. (1998) 'Confidentiality limits of managed care and clients' willingness to self-disclose', *Professional Psychology*: *Research and Practice*, Vol. 29, No. 6, pp.553–558.

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

Kuno, E., Hadley, T.R. and 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.

Lafferty, L. (2007) 'Medical identity theft: the future threat of health care fraud is now', *Journal of Health Care Compliance*, Vol. 9, No. 1, pp.11–20.

Lambrinoudakis, C., Gritzalis, S., Hatzopoulos, P., Yannacopoulos, A.N. and Katsikas, S. (2005) 'A formal model for pricing information systems insurance contracts', *Computer Standards & Interfaces*, Vol. 27, pp.521–532.

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.

Lorence, D.P. (2003) 'Measuring disparities in information capture timeliness across healthcare settings: effects on data quality', *Journal of Medical Systems*, Vol. 27, No. 5, pp.425–433.

Lorence, D.P. and Richards, M. (2002) 'Variation in coding influence across the USA', *Journal of Management in Medicine*, Vol. 16, No. 6, pp.422–435.

Lorence, D.P., Spink, A. and Jameson, R. (2002a) 'Information in medical decision making: How consistent is our management?', *Medical Decision Making*, Vol. 22, pp.514–521.

Lorence, D.P., Spink, A. and Jameson, R. (2002b) 'Assessing managed care market variation in reports of coding accuracy', *Managed Care Quarterly*, Vol. 10, No. 4, pp.15–25.

Lounsbury, D.W., Reynolds, T.C., Rapkin, B.D., Robson, M.E. and Ostroff, J. (2007) 'Protecting the privacy of third-party information: recommendations for social and behavioral health researchers', *Social Sciences and Medicine*, Vol. 64, pp.213–222.

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*, Vol. 76, pp.466–470.

Maglogiannis, I. and Zafiropoulos, E. (2006) 'Modeling risk in distributed healthcare information systems', *Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, New York City, NY, pp.5447–5450.

Magnusson, R.S. (2004) 'The changing legal and conceptual shape of health care privacy', *Journal of Law, Medicine and Ethics*, Vol. 32, No. 4, pp.680–691.

Malin, B. (2007) 'A computational model to protect patient data from location-based re-identification', *Artificial Intelligence in Medicine*, Vol. 40, pp.223–239.

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, pp.320–324.

Mandl, K.D., Szolovits, P. and Kohane, I.S. (2001) 'Public standards and patients' control: How to keep electronic medical records accessible but private', *British Medical Journal*, Vol. 322, No. 7281, pp.283–287.

Mercuri, R.T. (2004) 'The HIPAA-potamus in health care data security', *Communications of the ACM*, Vol. 47, No. 7, pp.25–28.

Messmer, E. (2008) *Health Care Organizations see Cyber Attacks as Growing Threat*, InfoWorld, February 28, http://www.infoworld.com/d/security-central/health-care-organizations-see-cyberattacks-growing-threat-801

Miller, A.R. and Tucker, C.E. (2009) 'Privacy protection and technology diffusion: the case of electronic medical records', *Management Science*, Vol. 55, No. 7, pp.1077–1093.

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, pp.202–207.

Muralidhar, K. and Sarathy, R. (2005) 'An enhanced data perturbation approach for small data sets', *Decision Sciences*, Vol. 36, No. 3, pp.513–529.

Myers, M.D. (1997) 'Qualitative research in information systems', *MIS Quarterly*, Vol. 21, No. 2, p.241.

National Research Council (NRC) (1997) *For the Record: Protecting Electronic Health Information*, National Academy Press, Washington DC.

Nepal, S., Zic, J., Jaccard, F. and Kraehenbuehl, G. (2006) 'A tag-based model for privacy preserving medical applications', in Grust, T., Höpfner, H., Illarramendi, A., Jablonski, S., Mesiti, M., Müller, S., Patranjan, P., Sattler, K., Spiliopoulou, M. and Wijsen, J. (Eds.): *Current Trends in Database Technology – EDBT Workshop*, pp.433–444.

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.

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.

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.

Ohno-Machado, L., Silveira, P.S.P. and Vinterbo, S. (2004) 'Protecting patient privacy by quantifiable control of disclosures in disseminated databases', *International Journal of Medical Informatics*, Vol. 73, Nos. 7–8, pp.599–606.

Peyton, L., Hu, J., Doshi, C. and Seguin, P. (2007) 'Addressing privacy in a federated identity management network for e-health', *Proceedings of the 8th World Congress on the Management of eBusiness*, Toronto, Canada, pp.12–12.

Poindexter, J.C., Earp, J.B. and Baumer, D.L. (2006) 'An experimental economics approach toward quantifying online privacy choices', *Information Systems Frontier*, Vol. 8, pp.363–374.

Poon, E.G., Cina, J.L., Churchill, W., Patel, N., Featherstone, E., Rothschild, J.M., Keohane, C.A., Whittermore, A.D., Bates, D.W. and 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.

Psaty, B.M., Boineau, R., Kuller, L.H. and 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.

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.

Raghupathi, W. and Kesh, S. (2007) 'Interoperable electronic health records design: towards a service-oriented architecture', *e-Service Journal*, Vol. 5, No. 3, pp.39–57.

Raman, A. (2007) 'Enforcing privacy through security in remote patient monitoring ecosystems', *6th International Special Topic Conference on Information Technology Applications in Biomedicine*, Tokyo, Japan, pp.298–301.

Ramsaroop, P. and Ball, M.J. (2000) 'A model for more useful patient health records', *MD Computing*, Vol. 17, No. 4, pp.45–48.

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*, Vienna, Austria, pp.318–324.

Reiss, S.P. (1984) 'Practical data-swapping: the first steps', *ACM Transactions on Database Systems*, Vol. 9, No. 1, pp.20–37.

Rindfleisch, T.C. (1997) 'Privacy, information technology, and health care', *Communications of the ACM*, Vol. 40, No. 8, pp.93–100.

Rosenberg, M.A. (1998) 'A statistical control model for utilization management programs', *North American Actuarial Journal*, Vol. 2, No. 2, pp.77–87.

Rosenberg, M.A. (2001a) 'A decision theoretic method for assessing a change in the rate of nonacceptable inpatient claims', *Health Services and Outcomes Research Methodology*, Vol. 2, No. 1, pp.19–36.

Rosenberg, M.A. (2001b) 'A statistical method for monitoring a change in the rate of nonacceptable inpatient claims', *North American Actuarial Journal*, Vol. 5, No. 4, pp.74–83.

Rosenberg, M.A. and Griffith, J.R. (2000) 'A management tool for controlling the rate of nonacceptable inpatient hospital claims', *Inquiry – Blue Cross and Blue Shield Association*, Vol. 36, No. 4, pp.461–470.

Rosenberg, M.A., Andrews, R.W. and Lenk, P.J. (1999) 'A hierarchical Bayesian model for predicting the rate of non acceptable in-patient hospital utilization', *Journal of Business and Economic Statistics*, Vol. 17, No. 1, pp 1-8.

Rosenberg, M.A., Fryback, D.G. and Katz, D.A. (2000) 'A statistical model to detect DRG upcoding', *Health Services and Outcomes Research Methodology*, Vol. 1, Nos. 3–4, pp.233–252.

Røstad, L. and Edsburg, O. (2006) 'A study of access control requirements for healthcare systems based on audit trails from access logs', *Proceedings of the 22nd Annual Computer Security Applications Conference*, Miami Beach, FL, pp.175–186.

Rothstein, M.A. and 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.

Samarati, P. (2001) 'Protecting respondents' identities in microdata release', *IEEE Transactions Knowledge and Data Eng*ineering, Vol. 13, No. 6, pp.1010–1027.

Sandhu, R.S., Coyne, E.J. and Youman, C.E. (1996) 'Role-based access control models', *IEEE Computers*, Vol. 29, pp.38–47.

Sankar, P., Moran, S., Merz, J.F. and Jones, N.L. (2003) 'Patient perspectives on medical confidentiality: a review of the literature', *Journal of General Internal Medicine*, Vol. 18, pp.659–669.

Schmidek, J.M. and Weeks, W.B. (2005) 'Relationship between tort claims and patient incident reports in the veteran health administration', *Quality and Safety in Health Care*, Vol. 14, No. 2, pp.117–122.

Schwartmann, D. (2004) 'An attributable role based access control for healthcare', in Bubak, M. (Ed.): *Proceedings of International Conference on Computational Science*, Kraków, Poland, pp.1148–1155.

Shen, J.J., Samson, L.F., Washington, E.L., Johnson, P., Edwards, C. and Malone, A. (2006) 'Barriers of HIPAA regulation to implementation of health services research', *Journal of Medical Systems*, Vol. 30, No. 1, p.65.

Sijs, H.V.D., Aarts, J., Vulto, A. and Berg, M. (2006) 'Overriding of drug safety alerts in computerized physician order entry', *Journal of Medical Informatics Association*, Vol. 13, pp.138–147.

Silverman, E. and Skinner, J. (2004) 'Medicare upcoding and hospital ownership', *Journal of Health Economics*, Vol. 23, pp.369–389.

Solomon, M.R. (2007) 'Regional health information organizations: a vehicle for transforming healthcare delivery', *Journal of Medical Systems*, Vol. 31, pp.37–47.

Sparrow, M.K. (1996) 'Health care fraud control understanding the challenge', *Journal of Insurance, Medicine*, Vol. 28, No. 2, pp.86–96.

Sparrow, M.K. (1998) *Fraud Control in the Health Care Industry: Assessing the State of the Art*, National Institute of Justice: Research in Brief, http://www.ojp.usdoj.gov/nij

Stingl, C. and Slamanig, D. (2008) 'Privacy-enhancing methods for e-health applications: How to prevent statistical analyses and attacks', *International Journal of Business Intelligence and Data Mining*, Vol. 3, No. 3, pp.236–254.

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.

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.

Susilo, W. and Win, K.T. (2007) 'Security and access of health research data', *Journal of Medical Systems*, Vol. 31, pp.103–107.

Swedlow, A., Johnson, G., Smithline, N. and 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, pp.1502–1506.

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.

Terry, N.P. and Francis, L.P. (2007) 'Ensuring the privacy and confidentiality of electronic health records', *University of Illinois Law Review*, pp.681–735.

Truta, T.M. and Vinay, B. (2006) 'Privacy protection: p-sensitive k-anonymity property', Paper presented at the *2nd International Workshop on Privacy Data Management*, 8 April, Atlanta, GA.

Truta, T.M., Fotouhi, F. and Barth-Jones, D. (2003a) 'Disclosure risk measures for microdata', *Proceedings of the 15th International Conference on Scientific and Statistical Database Management*, Cambridge, MA, pp.15–22.

Truta, T.M., Fotouhi, F. and Barth-Jones, D. (2003b) 'Privacy and confidentiality management for the microaggregation disclosure control method: disclosure risk and information loss measures', *Proceedings of the 2003 Workshop on Privacy in Electronic Society*, Washington DC, pp.21–30.

Truta, T.M., Fotouhi, F. and Barth-Jones, D. (2004a) 'Disclosure risk measures for the sampling disclosure control method', *Proceedings of the 2004 ACM Symposium on Applied Computing*, Nicosia, Cyprus, pp.301–306.

Truta, T.M., Fotouhi, F. and Barth-Jones, D. (2004b) 'Assessing global disclosure risk in masked Microdata', *Proceedings of the 2004 Workshop on Privacy in Electronic Society*, Washington DC, pp.85–93.

Turner, G. (2002) 'HIPAA and the criminalization of American medicine', *Cato Journal*, Vol. 22, No. 1, pp.121–150.

Tyler, J.L. (2001) 'The healthcare information technology context: a framework for viewing legal aspects of telemedicine and teleradiology', *Proceedings of the 34th Hawaii International Conference on System Sciences*, Maui, Hawaii, pp.6010.

USC – US Congress (2007a) *National Health Information Technology and Privacy Advancement Act of 2007*, S.1455, Legislation introduced on May 23, 2007, http://www.govtrack.us/congress/bill.xpd?bill=s110-1455

USC – US Congress (2007b) *Health Information Privacy and Security Act*, S.1814, Legislation introduced on July 18, 2007, http://www.govtrack.us/congress/bill.xpd?bill=s110-1814

USC – US Congress (2008) *Technologies for Restoring User's Security and Trust in Health Information Act of 2008*, H.R.5442, Legislation introduced on February 14, 2008, http://www.govtrack.us/congress/bill.xpd?bill=h110-5442

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.

Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W. and Middleton, B. (2005) 'The value of health care information exchange and interoperability', *Health Affairs*, Vol. 19, No. 1, pp.W5.10–W5.18.

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

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.

Warkentin, M., Johnson, A.C. and Adams, A.C. (2006) 'User interaction with healthcare information systems: Do healthcare professionals want to comply with HIPAA?', *Proceedings of the 12th Americas Conference on Information Systems*, Acapulco, Mexico, pp.2682–2691.

Wen, K.W. and Zhang, Y.J. (2002) 'Research issues on medical information systems facing the implementation of HIPAA', *International Journal of Healthcare Technology and Management*, Vol. 4, Nos. 1–2, pp.93–105.

Winkler, W.E. (2004) 'Masking and re-identification methods for public use microdata: overview and research problems', in Domingo-Ferrer, J. and Torra, V. (Eds.): *Privacy in Statistical Databases*, pp.231–246.

Woody, C. (2006) *Applying OCTAVE: Practitioners Report*, Technical Note, CMU/ SEI-2006-TN-010, http://www.sei.cmu.edu/reports/06tn010.pdf

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.

Zheng, Y., Chen, Y. and Hung, P.C.K. (2007) 'Privacy access control model with location constraints for XML services', *Proceedings of the 23rd International Conference on Data Engineering Workshop*, Istanbul, Turkey, pp.371–378.

Appendix 1: Classification of research in healthcare information security and privacy

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

*Categories** / *Articles*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
Threats to information privacy and security																
NRC (1997)	X															
Rindfleisch (1997)	X															
Etzioni (1999)		X	X													
Privacy concerns among healthcare consumers																
Sankar et al. (2003)			X													
Campbell et al. (2007)				X			X									
Angst et al. (2006)					X		X									
Bansal et al. (2007)					X		X									
Providers' perspectives of regulatory compliance																
Kaiser (2004)		X														
Kaiser (2006)		X														
Ness (2007)							X									
Inquilla et al. (2007)							X									
Warkentin et al. (2006)					X		X									
Miller and Tucker (2009)					X			X								
Information access control																
Rostad and Edsberg (2006)							X									
Ball et al. (2003)															X	X
Bhatti and Grandison (2007)											X	X				
Al-Nayadi and Abawjy (2007)												X				
Chen et al. (2005)												X				
Covington et al. (20000												X				
Schwartmann (2004)												X				
Ferreira et al. (2006)												X				
Malin and Airoldi (2007)												X			X	
Tentori et al. (2006)												X			X	X
Nepal et al. (2006)												X				X
O'Kefee et al. (2005)												X				X
Reidl et al. (2007)												X				
Li and Tripunitara (2006)										X	X	X				

*Categories** / *Articles*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
Information access control																
Motta and Furuie (2003)										X		X				X
Zhao and Johnson (2008)									X	X						
Data interoperability and information security																
AHRQ (2007a)	X															
AHRQ (2007b)	X															
Brailer (2005)		X														
Dogac et al. (2006)		X														
Eichelberg et al. (2005)		X	X													
Solomon (2007)	X			X												
Walker et al. (2005)								X								
Catley et al. (2004)												X				X
Estrella et al. (2004)												X				X
Raghupathi and Kesh (2007)												X				X
Information security issues of eHealth																
Ball, Gold (2006)			X	X												
Gallaher et al. (2002): NIST	X			X			X									
Hu et al. (2006): NIST	X	X											X			
Zheng et al. (2007)			X									X				
Peyton et al. (2007)				X								X				
Cheng and Hung (2006)													X			
Chowdhury and Ray (2007)													X			
Dong and Dulay (2006)													X			
Gold and Ball (2007)													X			
Hung (2004)												X				
Ramsaroop and Ball (2000)												X				
Information security for authorised data disclosure																
Behlen and Johnson (1999)		X														
El Emam (2008)		X														
Agrawal et al. (2004)												X		X		
Agrawal et al. (2002)		X										X				
Agrawal and Johnson (2007)		X										X				
Winkler (2004)		X	X													
El Emam and Jabbouri (2006)								X						X		
El Emam and Dankar (2008)								X		X				X		
El Emam et al. (2009)								X		X				X		
Hong et al. (2007)										X		X				

*Categories** / *Articles*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
Information security for authorised data disclosure																
Chao et al. (2005)										X	X	X		X		
Agrawal et al. (2007)										X	X			X		
Domingo-Ferrer et al. (2006)										X	X					
Domingo-Ferrer and Mateo-Sanz (2002)										X	X					
Samarati (2001)										X	X					
Malin (2007)					X					X	X					
Truta et al. (2007)					X					X	X			X		
Truta and Vinay (2006)					X					X	X					
Muralidhar and Sarathy (2005)										X	X					
Reidl et al. (2007)												X				
El Emam et al. (2007)							X									
Hasan and Yurcik (2006)								X								
Domingo-Ferrer et al. (2001)										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			
Susilo and Win (2007)										X						
Information integrity in healthcare and adverse effects																
Sijs et al. (2006)			X													
Aarts et al. (2004)				X	X											
Applebaum (2002)		X	X													
Walsh et al. (2006)				X			X									
Han et al. (2005)							X									
Koppel et al. (2005)							X									
Upperman et al. (2005)							X									
Poon et al. (2006)							X									X
Financial risk and fraud control																
Lefferty (2007)		X														
O'Malley et al. (2005)		X														
Sparrow (1996)		X														
Sparrow (1998)		X														
Becker et al. (2005)								X								
Silverman and Skinner (2004)								X								
CMS (2008)	X						X									

*Categories** / *Articles*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
Financial risk and fraud control																
FBI (2007)	X						X									
FORE (2005)	X						X									
Bolin and Clark (2004)	X							X								
Hillman et al. (1990)								X								
Swedlow et al. (1992)								X								
Lorence et al. (2002a)							X	X								
Lorence et al. (2002b)							X	X								
Lorence and Richards (2002)							X	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 and Griffith (2000)								X		X		X				
Johnson (2009)				X			X									
Regulatory implication to healthcare practice																
Cate (2002)		X														
Epstein (2002)		X														
Gostin and Hodge (2002)		X														
Hodge (2006)		X														
Hodge et al. (1999)		X														
Hodge and Gostin (2006)		X														
Lounsbury et al. (2007)		X														
Magnusson (2004)		X														
Mandl et al. (2001)		X														
Pumphrey et al. (2007)		X														
Terry and Francis (2007)		X														
Tyler (2001)		X														
Applebaum (2002)		X	X													
Baker (2006)		X	X													
Shen et al. (2006)				X												
Solomon (2007)		X		X												
Hyman (2002)		X						X								
Rothstein and Talbott (2007)		X						X								
Finne (1996)		X													X	
Gostin et al. (2001)		X										X				

*Categories** / *Articles*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
Information security risk management																
Woody (2006)	X															
Lambrinoudakis et al. (2005)										X						
Maglogiannis and Zafiropoulos (2006)										X						
Alberts and Dorofee (2003)												X				
Caralli et al. (2007)												X				
Poindexter et al. (2006)														X		