Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Human Error and Privacy Breaches in Healthcare Organizations: Causes and Management Strategies

Divakaran Liginlal
University of South Alabama, dliginlal@gmail.com

Inkook Sim
University of Wisconsin, inkook@gmail.com

Lara Khansa
Virginia Tech, larak@vt.edu

Paul Fearn
Memorial Sloan-Kettering Cancer Center, fearnp@mskcc.org

Follow this and additional works at: http://aisel.aisnet.org/amcis2009

Recommended Citation
Liginlal, Divakaran; Sim, Inkook; Khansa, Lara; and Fearn, Paul, "Human Error and Privacy Breaches in Healthcare Organizations: Causes and Management Strategies" (2009). *AMCIS 2009 Proceedings*. 406.
http://aisel.aisnet.org/amcis2009/406

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Human Error and Privacy Breaches in Healthcare Organizations: Causes and Management Strategies

Divakaran Liginlal
University of South Alabama
dliginlal@gmail.com

Inkook Sim
University of Wisconsin, Madison
inkook@gmail.com

Lara Khansa
Virginia Tech
larak@vt.edu

Paul Fearn
Memorial Sloan-Kettering Cancer Center
fearnp@mskcc.org

ABSTRACT

We apply Reason's GEMS typology to study privacy breach incidents in healthcare organizations. An interpretive analysis of transcripts of interviews with privacy officers of healthcare organizations in the U.S. Midwest helps discern the underlying causes of human error and develop a framework for error management. The study finds that organizational factors causing human error constitute a greater impediment to HIPAA Privacy Rule compliance than do human factors.

Keywords

HIPAA Privacy Rule, human error, mistakes, slips, organizational factors.

INTRODUCTION

The *Standards for Privacy of Individually Identifiable Health Information*, also known as the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA), established a set of national standards for the protection of certain health information (U.S. Department of Health & Human Services, 2006). These standards address the use and disclosure of individuals' health information ("protected health information") by organizations ("covered entities"), subject to the Privacy Rule, as well as standards for individuals' privacy rights to understand and control how their health information is used. A major goal of the Privacy Rule is to ensure that individuals' health information is properly protected, while still allowing the flow of information needed to provide and promote high quality health care and protect the public's health and well being.

Reason (1992) defined error as "the failure to achieve an intended outcome in a planned sequence of mental or physical activities when failure is not due to chance." On the other hand, a malicious act is also intentional but does not occur by chance and is directed at causing harm. Humans commit error often in ignorance and sometimes despite a strong determination to avoid it (Senders and Moray, 1991). Besides Reason (1992), Norman (1988) and Senders and Moray (1991) are good references for research on the topic of human error. Liginlal, Sim and Khansa (2009) investigated publicly-reported privacy breach incidents in the U.S. and determined that human error caused a majority of privacy breaches. They proposed a defense-in-depth strategy founded on error avoidance, error interception, and error correction. They also found that mistakes in the information processing stage constitute the majority of human error-related privacy breach incidents, clearly highlighting the need for effective policies and their enforcement in organizations. Kraemer and Carayon (2007) also studied human error and its effect on information security. They proposed a conceptual framework for examining the human and organizational factors contributing to information security breaches. Their lessons learned have implications on the cases of human error and privacy breaches. These previous studies, however, did not specifically focus on either the issue of medical privacy or the specific organizational context that caused the error. We fill this gap by addressing the following research questions in this paper:

1. What are the causal factors underlying human error that lead to Privacy Rule noncompliance?
2. What operational strategies and measures based on the identified causal factors can help manage errors that adversely impact HIPAA Privacy Rule compliance?

STUDYING THE NATURE OF HUMAN ERROR IN HEALTHCARE ORGANIZATIONS

The GEMS Model of Human Error

Reason (1992) categorized error into slips and mistakes. Slips occur as an outcome of the incorrect execution of a correct action sequence, while mistakes occur as an outcome of the correct execution of an incorrect action sequence, i.e., when an actor makes a wrong decision but executes it correctly. Mistakes also known as "planning failures" or "errors of intention," result from faulty conceptual knowledge, incomplete knowledge, or incorrect action specification. Slips are "execution failures" often arising from an actor's lack of skill, confusion, or loss of activation, as in the case of forgetting the original intention. The term 'lapse' is used by Reason to denote "an omission to execute an action as planned, due to a failure of memory." We consider the term 'slip' encompasses 'lapse' for the purpose of our analysis.

To gain a better understanding of the nature of human error in organizations, we extend our analysis beyond the GEMs model and adopt a more profound theoretical basis such as the taxonomy of medical error of Zhang, Patel, Johnson and Shortliffe (2002). Prior research conducted in human psychology has demonstrated that the tendency for error is strongly influenced by adverse conditions of work. These conditions include employee stress, fatigue, time pressure, cognitive overload, understaffing, difficult-to- execute procedures, inadequate supervision, poor communication, rapid changes within an organization, and systems design or implementation flaws (Berner and Moss, 2005). Studying these causal factors from an organizational perspective provides insights into the nature and types of error, the extent of their impact, and techniques to prevent or mitigate this impact. The study will also help gauge the importance that healthcare organizations attribute to human error as a cause of privacy breaches and identify the measures that are currently adopted by these organizations to remedy these underlying causes.

Research Design

HIPAA requires healthcare organizations to designate privacy officers whose primary responsibilities include tracking the use of PHI, setting up complaint procedures and punitive action guidelines, and developing overall HIPAA policies and procedures. Besides keeping up with the latest privacy practices, privacy officers also frequently supervise operations and training. In effect, a privacy officer is the driving force behind enforcing HIPAA compliance in a healthcare organization and is, as such, the best source of information about organizational practices and compliance history. Although privacy officers vary in their educational backgrounds, level of understanding of privacy and security concepts, and skills in policy analysis and decision making, their invaluable experience allows them to effectively comprehend how human error causes HIPAA privacy breaches.

Two privacy officers, with close ties to the University to which one of the researchers is affiliated, served as experts assisting our research design. Based on a preliminary review of the literature (Bogner, 1994; Moray, 1994; Vincent and Bark, 1995; Vincent and Taylor-Adams, 1998; Welker and Podleski, 2003) and the assistance of these experts, we developed a semi-structured interview questionnaire. The experts proved to be very reliable sources of information and their assistance proved invaluable for developing and refining the questionnaire and for obtaining contact information of key informants for the interviews. The introductory part of the questionnaire served to understand the background of the organization, and gauge the interviewee's depth of experience in HIPAA administration, particularly Privacy Rule compliance. The second part of the questionnaire was divided into three sections designed to uncover evidence related to human error as a significant cause of HIPAA privacy breaches and to understand their underlying causes, impact, and management. The influence of organizational factors, specifically understaffing, high turnover, low morale, and high workload, work environment, and task factors, and the effect of the knowledge and skill levels of employees on the likelihood of human error were considered in constructing the questionnaire. The first section was designed to evaluate the extent of human error as a cause for privacy breaches and the interviewee's assessment of the relationship between the employees' skill levels and the frequency of error occurrences. The interviewee was also required to recount specific privacy breach incidents that occurred in his/her organization. The second section aimed to categorize the causes and understand the impact of human error compared to other forms of threats causing privacy breaches. The questions were designed to study the differences, in magnitude and impact, among various human error types, i.e., slips and mistakes, in a healthcare setting. Particular care was taken, while designing this part of the questionnaire, to instruct the interviewees not to give emphasis on human error as a direct cause of HIPAA privacy breaches, but instead focus on the human and environmental factors that cause the errors leading to these breaches. The third section examined the management's priority to combat human error and the resulting privacy breaches through executing better strategies and dedicating more resources.

Research Methods and Interview Protocol

We compiled a list of privacy officers for our interviews from two states in the U.S. Midwest by searching the websites of the State Bar associations, the HIPAA-Collaborative, a joint effort of healthcare organizations designed to build a platform for implementing HIPAA, and the websites of leading healthcare organizations in the region. The experts who helped us with our research design also provided further contact information and leads. We sent out an initial request soliciting participation in our research to 25 large and medium-sized healthcare organizations in the two states. Only 14 privacy officers responded to our initial request for an interview. The informants were then contacted individually, briefed about the objectives of the study, and educated about the broader impacts of the proposed study. Not surprisingly, we found that the privacy officers were extremely reluctant to participate due to the confidential nature of the subject. Multiple follow up requests and written confidentiality agreements were required to obtain these officers' consent to participate. Finally, only 9 privacy officers agreed to participate in a one-hour interview. Teams of two researchers conducted 7 face-to-face interviews, each lasting about an hour, at the officers' work places. Due to schedule and logistical problems, 2 other interviews were conducted by telephone, also using two researchers. The interviews were conducted over a three month period. The privacy officers represented three medium-sized hospitals with 500 to 700 beds and multiple primary clinics, two large academic health systems affiliated to large Midwestern universities, and two large medical centers comprising a hospital, pharmacy, and health centers. Given the qualitative nature of the study, the 9 in-depth interviews provide a good representative sample for interpretive analysis (American Hospital Association, 2007).

Not only did the interview protocol require privacy officers to relate human error to HIPAA privacy breaches, but, as importantly, it also encouraged their creative and contextual thought process related to the avoidance, interception, and mitigation of human error. The interview questions purposefully avoided emphasis on terms such as mistake and slip, instead, using words with close meaning, such as inadequate knowledge (mistake) and poor skill or lapse of concentration (slip). The attempt was to facilitate an early inquiry of the informant's general perception of human error as a threat to HIPAA privacy breaches. To stimulate contextual thinking, the team asked the interviewees to relate their experiences in managing human error-related issues to subsequent drafting of policies or action plans. Open-ended questions, prompting interviewees at appropriate instances of the interview, were used to capture additional ideas. An example of such prompting is the illustration of human error as arising from lack of knowledge or poor execution. Three vignettes corresponding to skill-based and knowledge-based errors in the SRK framework, created in consultation with our two experts, served to illustrate the likely causes of human error. Upon conclusion of the interviews, team members transcribed their notes, organized by question, into a text-only electronic format. The notes from the two researchers who participated in each interview were combined, and any discrepancies in their notes were resolved with the help of a third researcher. Approximately a week after each interview, a follow-up questionnaire was mailed to the corresponding interviewees to probe them for additional thoughts that they failed to articulate during the interview. The study team then combined and contrasted the findings from the literature review and the key informant interviews to identify areas of overlap, agreement, or disagreement. To protect anonymity and provide confidentiality, no interviewee names were recorded in any document, be it hard or soft.

THE NATURE OF HUMAN ERROR IN ORGANIZATIONS: AN INTERPRETIVE ANALYSIS

The key informants had an average experience of 2.2 years in their current respective organizations, in addition to prior related policy-making experience in other organizations. As expected, all showed good understanding and in-depth knowledge of the Privacy Rule and the organizational activities impacting privacy. Although HIPAA regulations were considered very difficult to implement for various reasons, there was general satisfaction about the state of HIPAA compliance. The importance of translating the regulatory wording of HIPAA to a practically operational language was repeatedly emphasized. The most surprising finding was a general consensus that more than 90% of HIPAA privacy breaches are unintentional and non malicious, thus indicating that human error, whether mistakes or slips, constitutes the most significant threat to privacy. All the studied organizations put policies in place to prevent and rectify human error-related issues causing privacy breaches. Most of the privacy officers neither demonstrated an a priori understanding of the cognitive underpinnings of human error as a cause of privacy breaches nor did they appear to have taken the initiative to find systemic solutions to manage error in their respective organizations.

The Nature of Human Error

1. *Human error as a cause of Privacy Rule noncompliance*. The number and frequency of human error compared to other type of threats are very high, but intentional acts seem to be more damaging. Some privacy officers did not identify privacy breaches from a human error perspective. Instead, they have approached the issue from an event or process-based view. However, when prompted with examples of different categories of human error, they agreed they were able to isolate and categorize issues related to human error, which helped them understand and rectify the issue more easily.

2. *Comparison of human error to other threats*. Compared to unintentional acts, only a relatively limited number of intentional and malicious threats have been encountered by the officers during their tenure. Some felt that it was hard to accurately measure the frequency of errors since, unless the errors brought negative consequences, they were not likely to be noticed by managers and, even if noticed, errors were likely to be ignored.
3. *Relation between skills and human error*. There was no consensus as to whether or not employee skill is a major determinant of error. Unskilled employees may make more mistakes due to lack of knowledge; skilled employees are likely to have more responsibilities and information overload, and will, thus, tend to commit more slips. However, lack of knowledge is considered a more significant cause of human error compared to lack of skill or work ethic.
4. *Mistake vs. slip*. Errors arising from inadequate knowledge (mistake) rather than poor skills or lapse of concentration (slip) are the most damaging. The results from analyzing the publicly reported incidents showed a similar trend.
5. *Actors:* Clinical staff are the most difficult to work with, when it comes to enforcing privacy compliance, compared to administrative staff and third parties, such as contract employees. Clinical staff also tend to commit errors more frequently. This may arise from the cognitive overload, time pressure, and stress factors that clinical staff face in their day-to-day decision making activities (Gladwell, 2005). The clinical staff have too many competing priorities and when it comes to saving lives; privacy compliance tends to be less important. Managing clinical staff is, therefore, a high priority for Privacy Rule compliance.

Causes and Management of Error

We had originally identified eight primary causes of human error based on our literature review and in consultation with our two experts. The privacy officers (judges) were asked to rank order these causes based on what they perceived to impact compliance to the Privacy Rule most. In Table 1, we show the results of fitting the Rating Scale Model (Andrich, 1978) on the ranking data, using (Winstep, 2003) and assuming equal ordered thresholds for all items across judges, i.e., every judge used the equal distance ranking upon rating (Embretson and Reise, 2000).

Perceived Cause of Human Error	**Raw score**	**Measure**	**SE**	**Resulting Priority**
Lack of knowledge of Privacy Rule requirements	38	59.09	4.62	4
Poor discipline (e.g., laziness, arrogance, indifference)	44	47.1	4.39	5
Poor skills (e.g., computing skills, communication skills, work-related skills)	53	27.39	5.17	6
Inefficient business process and workflows (e.g., redundancy, bottleneck, not optimized)	18	96.55	3.95	2
Physical environment limitations (e.g., small rooms where everyone can overhear, etc.)	65	-4.77	5.29	7
Technology limitations (e.g., outdated computer applications, underpowered PCs, slow network)	69	-18.08	6.6	8
Organizational limitations (e.g., understaffed, high turnover, low morale, high workload, etc.)	14	103.76	4.69	1
Poor monitoring and enforcement (e.g., little incentives or penalties)	23	88.97	3.94	3
INPUT: 9 Judges 8 Items MEASURED: 9 Judges 8 Items 8 CATS Judge: REAL SEP.: .00 REL.: .00 ... Item: REAL SEP.: 8.55 REL.: .99				

Table 1. Results of Rasch Analysis on the Ranking of Causes of Error

Table 1 shows the computed measures and priorities for each item, as well as the separation and reliability of items and judges. Separation and reliability measure the degree to which the items (or judges) differentiate judges (or items) on the measured variables. The separation index and reliability are 0 for judges due to the fact that the measured variables constitute ranking data and the resulting total scores are the same across judges. The item separation index and reliability are 8.55 and .99, respectively, indicating high separation (i.e., > 2.0) and good reliability (i.e., > .80). Organizational limitations were

identified as the primary cause of human error followed by poor monitoring and enforcement and inefficient business processes and workflows. This suggests that officers consider human error as not just a people issue, but, more importantly, as stemming from the work environment. Further, addressing the inefficiencies in business processes, improving workflows, and monitoring and enforcing policies are also considered important. Interestingly, technology limitations as a cause of human error received the lowest ranking. A summary of the recommendations made by the privacy officers for addressing each cause of human error leading to Privacy Rule noncompliance is shown in Table 2. Clearly, many of the causes of error, including the top two, cannot be solely addressed by the privacy officers, and require strong support from both operations and upper management. Organizations appear to have more difficulty in managing systemic causes because these causes are harder to diagnose and require more time, money, and management involvement to fix.

Perceived Cause of Error	Priority	Suggested Measures
Organizational limitations (e.g., understaffed, high turnover, low morale, high workload, etc.)	1	Analysis of workflows and changes designed to reduce the individual's workload, active upper management involvement in policy directives and their enforcement.
Inefficient business process and workflows (e.g., redundancy, bottleneck, not optimized)	2	Reengineered processes and change management, active upper management involvement in policy directives and their enforcement.
Poor monitoring and enforcement (e.g., little incentives or penalties)	3	Auditing, leadership training.
Lack of knowledge of Privacy Rule requirements (e.g., policies, procedures, protocols)	4	Privacy training for all employees, continuous reminders, education, periodic updates based on issues
Poor discipline (e.g., laziness, arrogance, indifference)	5	Enforcement, consistent disciplinary actions, better supervision (Mostly an HR issue)
Poor skills (e.g., computing skills, communication skills, work-related skills)	6	Training, clearly defined policies in the employee manual
Physical environment limitations (e.g., small rooms where everyone can overhear, etc.)	7	Remind people of the limitations and how to avoid possible issues. Action in concert with facility manager.
Technology limitations (e.g., outdated computer applications, underpowered PCs, slow network)	8	Resource availability, good IT policies

Table 2. Recommendations by Privacy Officers for Managing Human Error

MANAGING HUMAN ERROR FOR HIPAA COMPLIANCE

In this section, we analyze the strategies for error management suggested by the privacy officers and attempt to develop a comprehensive framework by referring to the related literature, industry best practices for managing medical errors.

Building a Framework for Error Management

Our study suggests that the top three causes of human error leading to privacy breaches arise from organizational factors. All privacy officers believed that active upper management involvement in policy directives and enforcement, and careful examination and reengineering of workflows were the most important error management strategies. Human factor issues ranked second to organizational issues, while technology-related issues ranked the lowest. Periodic training and awareness programs were identified as the primary techniques for addressing human factors. IT policies and resource availability of new technologies were identified as methods to address technology limitations.

A number of studies motivated by the Institute of Medicine's report on medical errors (Institute of Medicine, 2000; Institute of Medicine, 2001) have attempted to identify the important dimensions of medical error management (Lenert and Bakken, 2002; Patel and Bates, 2003). In their study of the cognitive factors underlying medical errors, Zhang et al. (2002) started out by examining the sources of errors from a hierarchical perspective. At the core are individuals who trigger errors, without

necessarily being the root cause of these errors. The higher levels in the hierarchy are human-computer interaction, such as interactions among individuals, and between groups of people and technology; organizational structures such as coordination and communication; institutional functions such as policies and guidelines; and the national regulatory regimes. The objective of the study was not to examine the six levels independently, but to build a cognitive foundation at the level of the individuals and their interactions with technology.

The Institute for Safe Medication Practices (ISMP, 2002) recommends incorporating error management into a healthcare organization's strategic plan, proactively identifying error-prone processes, and devising safe alternatives using process flow analysis to combat medication errors. Further, the Institute (ISMP, 1999) suggests the following measures ranked in order of priority to remedy medication errors: forcing functions and constraints that result in designing processes so that errors are virtually impossible or difficult to make, simplification and standardization of procedures, reminders, checklists, and double check systems, rules and policies to support error prevention and disciplinary measures for errant actions, and enhanced education and awareness. A recent study of four hospitals (McFadden and Towell, 2004) identified seven critical success factors for reducing the likelihood of medical errors or minimizing their effects. The most important factors are changing the organizational structure, causal analysis and redesigning processes and systems as required, changing the organization's safety culture, focusing on the process and not the individual, and education and training. Based on the results of our interviews, we developed an error management framework to address HIPAA Privacy Rule breaches.

Error Management Strategies for HIPAA Compliance

Slips in general can be reduced through better training to enhance employee skills. Mistakes can be reduced by improving employee knowledge through education and awareness programs. Given that human beings are fallible and errors do happen, any effective error management framework must also embrace the external factors that cause or accentuate human error. The error management strategies resulting from our study, therefore, address three dimensions: organizational, human, and technological. Table 3 depicts the strategies and measures across the three dimensions.

Organization-focused strategies include implementing stringent administrative measures, reengineering workflows, and creating better work environments aimed at facilitating both preventive and corrective cognitive interventions. Besides training employees, most forms of slips can be addressed by improving organizational workflows and providing technological support. Similarly, mistakes can be addressed by instituting better administrative measures, such as effective policies, guidelines, and disciplinary measures. Privacy impact assessments help identify areas of noncompliance, assess risks, and evaluate alternate safeguards. Incident handling procedures must not only be aimed at preventing the escalation of a breach but should incorporate causal analysis. The blame game should be avoided, a culture of prompt reporting and analysis of errors should be promoted, and disciplinary actions, if any, must serve as deterrents. Technology-focused strategies aim at providing cognitive enhancements for better decision aiding and enhanced situation awareness.

Implementing a robust information security program with clear organizational guidelines about remote computer use is what this paper is focusing on. Organizations need to disallow offsite use of, or access to PHI unless specifically warranted, in which case suitable safeguards and employee training need to be ensured. Further, organizations need to limit the collection of personal information, to reduce the opportunity for that information to be compromised. An important best practice is to disallow the retention of personal data longer than needed, thus eschewing the risks of the data being compromised. Only individuals with a need to access sensitive information should have such access, and protective measures need to be put in place to monitor that access. To address the problem of loss of critical data the HHS suggests processes to ensure backup of all data entered into remote systems with policies to encrypt such backed up data. Further, there should be procedures in place for deleting sensitive information and disposing of media containing such information.

CONCLUSIONS, LIMITATIONS, AND FUTURE RESEARCH

Liginlal et al. (2009) studied human error as a major cause of privacy breach incidents in the U.S. and proposed a defense-in-depth strategy based on principles of error avoidance, error interception, and error correction. The study concluded that mistakes in the information processing stage are associated with the majority of human error-related privacy breach incidents, clearly highlighting the need for effective policies and their enforcement in organizations. However, the study did not examine the impact of errors in the HIPAA context nor did it analyze the underlying organizational processes that cause human error. In this paper, we categorized human error based on Reason's GEMS typology, and Zhang et al.'s (2002) taxonomy of human error. The semi-structured interviews with privacy officers of healthcare organizations reinforced this finding and facilitated a good understanding of the causal issues - both organizational and human-related. Clinical staff tend to commit more errors leading to privacy breaches. However, understandably so, privacy officers noted the need for more practical and efficient privacy policies that give clearer guidelines to clinical staff on how to avoid violating the Privacy Rule.

The important contribution of this paper lies in developing a practical framework to address human error as a key factor in Privacy Rule compliance and a major cause of HIPAA privacy breaches.

One expectation for computerized systems is that they can replace human workload and minimize errors. To some degree, this expectation is materialized especially for repetitive tasks. On the other hand, as more computerized systems are used, human workers become responsible for task management and decision making, and errors made at that level can have severe consequences. It is also important to study organizational workflows to identify the conditions under which errors occur and effectively mitigating factors, such as fatigue, stress, and time pressure. Our ongoing research consists of focusing on studying the differences among the methods of enhancing situation awareness and forcing functions for the effective management of human error in the context of privacy.

Dimension	**Strategies**	**Measures**
Organization-focused	Incorporate stringent administrative measures	Effective security program, privacy policies, and operational guidelines Adoption of best practices
		Privacy impact assessment
		Incident handling procedures
		Disciplinary action (Sanction policy)
	Reengineer organizational workflows	Reduce multitasking, goal stacks
		Manage distractions, crew turnover, time pressures, reduce stress and fatigue
		Increase automation
		Manage information overload
		Checks in workflow
	Provide a conducive work environment	Standardize workspace design, reduce possibility of overhearing
Human-focused	Develop employee skills	Provide periodic training
		Develop supervisory skills
		Test employee skills
	Improve employee knowledge	Provide education on a regular basis
		Test employee understanding of policies, standards, and best practices
	Promote safety culture	Awareness programs, incentives for prompt reporting and analysis of errors
Technology-focused	Protect confidentiality of data	Strong authentication, encryption, patches and updates, antivirus, lockdown of devices
	Provide better decision aiding	Memory aids
		Visual, spatial, and other model and data representation aids
	Enhance situation awareness	Aid context awareness
	Use technology-based forcing functions	Intercept error

Table 3. Error Management Strategies and Measures

REFERENCES

1. American Hospital Association. (2007) Trendwatch chartbook, chapter 5: Workforce, available at http://www.aha.org.
2. Andrich, D. (1978) Rating formulation for ordered response categories, *Psychometrika*, 43, 561-573.

3. Berner, E.S. and Moss, J. (2005) Informatics challenges for the impending patient information explosion, *J Am Med Inform Assoc*, 12, 6, 614-617.
4. Bogner, M.S. (1994) Human error in medicine, Hillsdale, NJ: Lawrence Erlbaum.
5. Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) The effect of internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers, *International Journal of Electronic Commerce*, 9, 70-104.
6. Embretson, S.E. and Reise, S.P. (2000) Item response theory for psychologists, Mahwah, NJ: Erlbaum.
7. M. Gladwell. (2005) Blink: The power of thinking without thinking, Little Brown and Company, NY.
8. ISMP. (1999) Medication error prevention toolbox, *Institute for Safe Medication Practices, Medication Safety Alert Newsletter*.
9. ISMP. (2002) Organizations release new tools for reducing medication errors, *Institute for Safe Medication Practices News Release*.
10. Institute of Medicine. (2000) To err is human: Building a safer health system, Washington, DC: National Academy Press.
11. Institute of Medicine. (2001) Crossing the quality chasm: A new health system for the 21st century, Washington, DC: National Academy Press.
12. Kraemer, S. and Carayon, P. (2007) Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists, *Applied Ergonomics*, 38, 2, 143-154.
13. Lenert, L.A. and Bakken, S. (2002) Enabling patient safety through informatics: Works from the 2001 AMIA annual symposium and educational curricula for enhancing safety awareness, *J Am Med Inform Assoc*, 9, 6, S1–S132.
14. Liginlal, D., Sim, I. and Khansa, L. (2009) Human error and its impact on information privacy, *Computers and Security*, forthcoming.
15. McFadden, K.L., Towell, E.R. and Stock, G.N. (2004) Critical success factors for controlling and managing hospital errors, *Quality Management Journal*, 11, 1, 61-64.
16. Moray, N. (1994) Error reduction as a systems problem, in: Bogner, M.S. ed. Human error in medicine, Hillsdale, NJ: Lawrence Erlbaum, 67-92.
17. Norman, D.A. (1988) The psychology of everyday things, New York: Basic Books.
18. Patel, V.L. and Bates, D.W. (2003) Cognition and measurement in patient safety research - Guest editorial, *J Biomed Inform*, 36, 1–2, 1–3.
19. Rasmussen, J. (1983) Skills, rules, knowledge; signals, signs, and symbols, and other distinctions in human performance models, *IEEE Transactions on Systems, Man and Cybernetics*, 13, 257-266.
20. Reason, J. (1992) Human error, Cambridge, UK: Cambridge University Press.
21. Senders, J. and Moray, N. (1991) Human error: Cause, prediction, and reduction, Lawrence Erlbaum Associates, Hillsdale, NJ.
22. U.S. Department of Health & Human Services. (2006) HIPAA security guidance, **available at** http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf.
23. Vincent, C.A. and Bark, P. (1995) Accident investigation: discovering why things go wrong, in: Vincent CA, ed. Clinical risk management, London: BMJ Publications, 391-410.
24. Vincent, C.A., Taylor-Adams, S. and Stanhope, N. (1998) Framework for analyzing risk and safety in clinical medicine, *British Medical Journal*, 316, 1154-7.
25. Welker, I. and Podleski, J. (2003) Not yet compliant with HIPAA privacy rules? *Nursing Economics*, 21, 6, 291-295.
26. Winsteps [Computer software]. (2003) Rasch measurement software and publications, available at http://www.winsteps.com.
27. Zhang, J., Patel, V.L., Johnson, T.R. and Shortliffe, E.H. (2002) Toward an action based taxonomy of human error in medicine, in *Proceedings of the Twenty-Fourth Annual Conference of the Cognitive Science Society*, 970–975.