Risk Management For Health Information Security And Privacy

Mirza B. Murtaza, Middle Tennessee State University, USA

ABSTRACT

The challenge of securing large amounts of electronic medical records stored in a variety of forms and in many locations, while still making it available to authorized users, is huge. Pressure to maintain privacy and protection of personal information is a strong motivating force in the development of security policies. It is essential for health care organizations to analyze, assess and ensure security policies to meet these challenges and to develop the necessary policies to ensure the security of medical information.

Keywords: Electronic Health Information; Electronic Health Records; Risk Management

INTRODUCTION

An individual's health care information is personal and considered private. The field of health informatics has been given added significance over the last few years with the emergence of electronic health information (EHI) and patients' individual electronic health records (EHR), in particular. Implementation of EHR has also been suggested as a means to facilitate health care system redesign in order to improve quality of care and productivity (Evans, Nichol and Perlin, 2006). It has been suggested that the major issues relevant to EHR are cost savings from implementation of HER, virtual networking and access to patient data remotely, Electronic Medical Records, source credibility and privacy concerns, and physician-patient relationships (Mukherjee and McGinnis, 2007). Virtual networking is a relatively new concept in the medical profession and physicians and other health-care providers can access information from any place and at any time. Electronic Medical Records (EMR) include patient charts and other records that were mostly kept in physical format prior to the introduction of electronic records and are essential for quality of care.

There are many factors that impact the way organizations deal with EHI and EHRs, including regulatory mandates from the Health Insurance Privacy and Portability Act (HIPPA) and the industry best practices. In addition to health-care providers (hospitals, physicians, laboratories and clinics), there are other industries that are involved in health-care delivery, such as pharmaceutical companies, insurance companies, and medical research institutions. All of these industries have legitimate business interests, but the impact on providing actual medical care is tangential, however, the impact on the volume of patient records is huge. The availability of data regarding patients and their conditions, treatments, and procedures will be beneficial to all of these organizations as well as to the public health organizations that work to prevent situations that are potentially epidemic and catastrophic. When available and linked properly, this data can be analyzed to track trends and link results to the care and medications prescribed. If complete medical histories are made available to primary and emergency care givers, they can potentially produce better care and improve care procedures.

It is possible that commercial entities might have a strong desire to access medical information, such as patient histories, along with procedures and treatments performed, that would allow them to direct resources to profitable health care areas and target patients who require the medications and treatments they market. This is a reasonable desire, but it will compromise patient privacy. Besides challenging society's privacy values, gaining access to full medical information for malicious purposes could result in a potential threat to the society. Medical information is valuable and its value continues to grow as the health care costs skyrocket. The pressure to acquire, review, study, or even steal information is growing. It seems that it may be only a matter of time until medical information was sold, just like mailing lists and shopping information are sold, and once information is out in the highly networked world, it is difficult to make it private again. Therefore, the challenge today is to maintain security, integrity, and availability of this very important information while dealing with the social and commercial pressures for privacy versus information sharing. The challenge begins with enforceable policies, rules, guidelines, and procedures and is followed by technical system solutions that have the usual data security issues.

TECHNOLOGICAL ISSUES

According to Health Information Management Systems Society (HIMSS), Electronic Health Record (EHR) is a longitudinal electronic record of patient health information that is generated by one or more encounters in any care delivery setting (hospital, clinic, doctor's office, lab, etc.) (NIH, 2006). Some of the potential information it can include is patient demographics, problems and conditions, medications, vital signs, medical history, immunization records, laboratory data, and radiology reports. In the past, each entity involved (hospital, pharmacy or lab) kept its own electronic health records; however, today an integrated architecture can be developed to allow sharing of data across different systems (NIH, 2006). Each system can store its own data locally, but to share patient information, a system has to allow another system to access its data storage. This, of course, requires some level of interoperability between the partner entities' systems.

Unfortunately, there is no single standard of EHR technology; a variety of standards and protocols exist that can be incorporated into a particular EHR system and customizable to a particular provider's work requirements. There are three main organizations that create standards related to EHRs. Within the US, Health Level Seven (HL7) develops the most widely used health care-related electronic data exchange standards. In Europe, Comite Europeen de Normalization – Technical Committee (CEN TC) 215 develops standards to be used within European nations. The third organization, American Society for Testing and Materials (ASTM) E31, is also involved in developing standards (in cooperation with HL7 and CEN TC) that are mainly used in commercial labs.

Most of the major professional health information associations, such as the American Health Information Management Association (AHIMA), the Health Care Information and Management Systems Society (HIMSS), and Health and Human Service's American Health Information Community (AHIC), have all tried to establish industry standards for health informatics with significant consideration given to the security of EHRs.

Health Level Seven (HL7) standard was established in 1987 and is dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, and the delivery and evaluation of health services. In a typical hospital, there are patient records, physician records, inventory systems, billing systems, payroll systems, etc. Since these systems were developed or acquired at different times, they are stored and managed using various specialized computer programs. Additionally, every medical clinic and testing lab uses its own information systems that may differ from other hospitals and clinics. To help communication and information exchange between these health care points, standards - like the ones developed by HL7 - are needed in order to make sure that information is passed correctly between health care providers.

Currently, more than 90% of all health care facilities in the United States use the HL7 standards, as well as hospitals in several other countries. The three main user groups for HL7 are clinical interface specialists, government entities, and medical informatics (Shaver, 2007). The current version of HL7 being used is the 3rd version - HL7 RIM (Reference Information Model). RIM is a collection of subjects, classes, events, attributes, use cases, actors, and interactions (Beeler, 2004). The structure of the RIM is based on six core classes - act, entity, role, participation, act relationship, and role link. The first two - act and entity - are considered the two major classes because entities are defined as all of the stakeholders in health care, and acts are the actions involving the stakeholders. The next two classes are role and participation. Role refers to the fact that an entity can assume one or more roles, such as registered nurse, patient, responsible party, etc., in the health care field. Participation refers to the participation in a given act by the entity who is assuming role/roles. Finally, the last two classes in RIM are role link and act relationships. Both of these classes refer to the ability to link two or more roles – or acts – together (Beeler, 2004).

RIM was not intended to be a model for a database or a logical design for a particular vendor's information system. It was not intended to represent a particular set of HL7 messages, but rather a reference model of data and relationships from which any relevant HL7 message could be developed. "Specific users of the RIM are expected to utilize relevant portions of it as needed, adopting its content to their own information modeling needs and notations." (Beeler, 2004) However, several problems have been identified with the implementation and continued use of the HL7 standards. Some of these problems include interoperability, usability in specialist domains, scope, documentation, and learning ability.

LEGAL AND COMPLIANCE ISSUES

EHRs have often been claimed as a major technological breakthrough in the health care field that would help improve efficiency and effectiveness of health care services. As early as 1993, the government proposed blue print identifying health information systems as critical in any system overhaul. Among the potential benefits of EHRs are the reduction of administrative paperwork and costly medical errors, easy access to a patient's comprehensive medical history, and the enhanced ability to view health information in ways that could improve patient diagnostics, public health outcomes, and minimize the chance of adverse drug interactions.

However, the widespread use EHRs would alleviate the concerns regarding patient privacy and confidentiality. There are numerous risks that a patient's electronic record could be hacked into, stolen, altered without authorization or improperly disclosed. Since few proposals have called for a centralized data warehouse for EHRs, many are concerned about the transmission of information and the possible interception by unauthorized third parties. Other major concerns pertain less to health information security and more to the scope of EHR adoption, such as the potential for an individual's health record to be used to discriminate against in employment, insurance, and so forth. To allay concerns about EHRs and protect privacy, the Independent Health Record Trust Act of 2007 gives patients full access to their EHRs, including the right to view their records, add their own comments to the file, and even potentially pass their EHRs along to future generations.

The growing volume of personal medical information and the shear amount of raw data will put pressure on the entire electronic storage system. Systems will have to control the source data to ensure accuracy and linkage to other relevant information. The data will be stored in multiple locations and linked to other destinations. Robust networks and new data warehouse technology will be needed to lock the data down but make it available. All of the usual electronic data storage security issues will apply in this case. The internet, distributed networks, storage technologies, record retention, access control, data conversions, application development, and many other issues come together to demand methodical and detailed plans to ensure that the security processes and systems perform as required. There is no absolute way of preventing determined humans, whether they are considered hackers or thieves, from attempting to access and use stolen health information.

There is major concern about how to protect this vast amount of data and information from a wide range of sources while ensuring the integrity of the data and making the information available to a very broad range of health care professionals, staff workers, and patients. Since individuals would demand the rights to privacy, there are some strong motivating forces that will help protect our private medical information, but it requires a vigilant oversight of the procedural, technical and physical systems that must be in place. The oversight that is needed in this area will provide the guidelines for how data are handled, accessed, and used and will provide the power to enforce the security.

There are a number of privacy issues that could be faced by consumers if their medical information is included in an HER, such as 1) privacy and integrity of health-related data, 2) security breaches, and 3) medical identity theft (Clarke et al., 2009). The HIPAA Privacy Rule provides federal protection for personal health information held by entities and provides patients' rights with respect to their information. A key to this rule is that it is balanced so that it permits the disclosure of personal health information when needed by a permitted authority. The security rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information.

Just like with any security issues (physical, procedural, technical), medical information is getting a lot of attention because of the broad scope, its importance, and the enormity of its impact if used in a harmful or malicious way. Anyone who handles or has access to medical information will require specific training for the respective responsibilities. HIPAA addresses the protection of patient records in all forms. New systems will be in place, as well as new processes and procedures; but primarily, the access, accuracy, and availability of the information must be protected.

Some argue that HIPAA alone does not go far enough to protect medical information because of perceived weaknesses in the enforcement of the guidelines. Other organizations define stricter guidelines, such as ISO 27799-2008. This standard augments the previous ISO 2005 standards and applies to all health information, and it addresses the use of internet and wireless technologies to share personal medical information and the need to better protect confidentiality. If followed, it would make information more secure; however, ISO is also limited in its enforcement power. While HIPAA is designed to protect privacy, it does not specify how that has to be done. HIPAA is not an information technology (IT) standard, so it does not specify means to protect data from an IT standpoint. This ISO 27799-2008 standard provides a standard for health organizations that they can use to adopt better IT security stance (ISO 27001, 2011). Standards organizations are developing or upgrading standards to address the challenges. These organizations look at security from different perspectives to try to establish general guidelines and specific techniques for maintaining secure data.

Oversight is complex and many organizations are beginning to acknowledge the need for coordinated programs. Several agencies have reviewed the current status of programs to address the information sharing issues and they reached similar conclusions. Recognizing the need to centralize control, the Secretary of Health and Human Services (HHS) delegated to the Director of OCR (Office for Civil Rights) the authority to administer and enforce the HIPAA security rule. Unfortunately, neither HHS nor OCR is a technologically advanced organization well-equipped to oversee the electronic health care development.

Currently, health information security is governed in the United States under the HIPPA legislation, adopted by the United States government in 1996. This legislation is chiefly concerned with the protection of Electronic Protected Health Information (EPHI). Under the regulatory powers of Health and Human Services, a framework has been developed that applies HIPPA to EHRs, with full implementation of the regulations to all covered entities that use EHRs.

The main objective of health information security is to assure the confidentiality, integrity, and availability of a covered entity's information system. This does not distinguish health information security objectives from those of other fields of endeavor outside of health care. What is particularly distinctive about health information security is the very low threshold reached before a given operation becomes critical to the functioning of a covered entity; patients' lives and well-being are, in a real sense, entrusted to the essential functioning of health care IT. While HIPPA is primarily concerned about the privacy and confidentiality of patient health records, one can say that the other goals of integrity and availability are complimentary to confidentiality. To that end, HHS in interpreting HIPPA as a standard three-pronged approach to health IT security, especially as it pertains to EHRs. The three main areas are administrative controls, physical controls, and technological controls. It is noteworthy that some of the controls are required whereas others, while seen as best practices, are addressable but not mandatory in any strict sense.

Administrative Safeguards

Administrative controls pertain to the organizational culture of a covered entity and how that entity perceives the importance of health information security. Under HIPPA, all information security policies should be in writing, with a designated privacy officer charged with oversight of HIPPA compliance. Mechanisms should be put in place to ensure effective management oversight of IT security. Employee involvement with trainings and periodic reminders about best practices can help raise the profile of IT security within the entity. Third-party vendors should be scrutinized for their compliance with HIPPA as a stipulation of doing business with the entity.

One best practice is to limit employee access to EHI to only those who need the particular information to effectively perform their job-related duties. Given the high growth in health care and the large number of personnel changes at many health organizations, policies should be in place to address authorization, establishment, modification, and termination of employee access to EHI as employees join the entity, have a change in job duties, or separate.

Finally, best administrative practices address the need for contingency plans. Risks should be identified and then addressed in terms of critical functionality to the entity. For example, the provisions must be in place in the event that there is a power outage while a patient is undergoing a life-saving operation. A provider may mandate that a paper copy of vital records are on hand for quick consultation should IT resources temporarily become inaccessible. Disaster recovery, incident response, and data backup provisions should be established, with periodic testing and appropriate modifications made as necessary. Activity on the health IT system should be logged and periodically audited on both a routine and event-based basis to ensure HIPPA compliance.

Physical Safeguards

An effective information security plan addresses the need to have a physically secure IT network, whether it is a central data storage facility or an end-user terminal. One of the more obvious, yet sometimes overlooked, considerations is the correct placement of terminals where they cannot easily be seen by passers-by. Physical security is also strengthened with restricted access of work areas to authorized personnel, the use of sign-in logs for visitors, and escorts to and from areas processing EHI.

Provisions should be made to limit software and hardware only to properly authorized individuals and carefully controlled monitoring of equipment with EHI, especially portable devices, such as laptop computers that might be misplaced or stolen. Various medical devices may not be components of the IT system yet may contain within them certain forms of EHI that should be handled in the appropriate manner. Controls should be in place for third-party vendor compliance, as well as accurate records for the installation or removal of any hardware and software from the IT network.

Technical Safeguards

Technological safeguards are central to ensuring the integrity of patient data in preventing unauthorized changes to information, breaches in IT network security, and ensuring that all users and disclosures are correctly authenticated. HIPPA provides that in an open network, encryption of EHI must be used, while this is optional in closed networks. The entity is ultimately responsible for ensuring that EHI is not altered in any unauthorized manner through means of strong passwords, digital signatures, integrity checks, etc. In disclosing EHI to outside parties, the entity should also establish a means of authentication by way of telephone call-backs, two or three-way handshakes, or token systems. HIPPA provides that all risk analysis and risk management should be documented, along with a comprehensive written record of all configuration settings and documentation of HIPPA compliance. Finally, provisions should be made for guarding an entity's IT system against threats to any IT system including viruses, malware, hacking, and denial of service (DoS) attacks.

RISK MANAGEMENT

The task to secure medical information encounters all of the usual technical obstacles. According to a General Accounting Office (GAO) report, emerging cyber-security issues threaten federal information systems. "Agencies' perceptions of the risks of spam, phishing, and spyware vary. In addition, most agencies were not applying the information security program requirements of the Federal Information Security Management Act of 2002 (FISMA) to these emerging threats, including performing risk assessments, implementing effective mitigating controls, providing security awareness training, and ensuring that their incident-response plans and procedures addressed these threats."

On an even larger scale, there are the usual logical and physical security threats, such as information theft, data corruption, data backup problems, power loss, user and operator errors, portable device misuse, network communications, and circumvention of procedure. As portable computing becomes more ubiquitous with systems, like tablet computers and laptops being used in hospitals, in ambulances, with doctors and other caregivers, inherent security problems occur. Data management always needs attention and the volume will demand more resources. Although most institutions are adequately prepared, smaller facilities and offices may not have adequate backup power or other resources to prevent data corruption.

Cloud computing or distributed processing and information sharing present a big problem for securing dynamic data that is intended to be widely accessed. Application design and implementation, internet use, network security, machine level security on individual diagnostic machine interfaces (MRIs and scans), digital x-rays, or any other equipment that stores or transmits data to a network will require new security systems and procedures. General and granular system security design must be strong and virtually every area of concern for security specialists must be reviewed and secured.

It is advisable that the individuals in charge of managing risk at health care institutions adopt a structured process for protecting the interests and resources of the organization. This process requires a continuous cycle (Figure 1) of identification of risks, assessment, actions and monitoring (Misra, Kumar & Kumar, 2007).

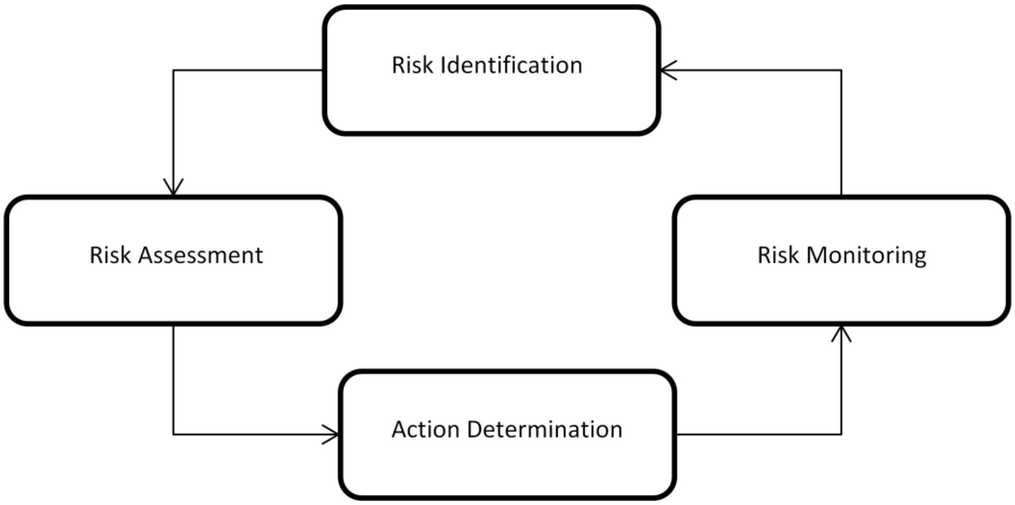

Figure 1: Risk Management Cycle

Table 1 outlines the elements of each step which are described as follows:

Risk Identification

The first step is to evaluate the organizational requirements, which are based on those set forth by legislation (like HIPAA), industry standards and best practices, and organizational policies. This would help determine the resources that must be protected. Databases and networks are the obvious resources, but the specific threats must be identified. An understanding of organization's IT infrastructure is essential – how the information flows through the systems would help ascertain the risks. It is also important to evaluate the impact of all vulnerabilities and how it would affect the confidentiality, integrity, and availability of the resource.

Risk Assessment

The next step is to assess the impact of each risk in either qualitative or quantitative terms. The risk assessment should not only evaluate each individual vulnerability, but also the interrelationships within them. For example, there is a certain level of threat against the database; however, along with an untrained user, it would become a bigger threat when an employee inadvertently releases some data.

Once the risks are assessed, risk reduction planning would ensue, resulting in a security action plan. The plan would highlight each person's responsibilities and the actions to be taken, steps that would be taken to mitigate the risk, and how the reporting of actions would be done.

Table 1: Risk Management Steps

1. Risk Identification • Regulatory and Standards compliance • Environment evaluation • Process and source identification • Risk identification	3. Action Determination • Risk Prioritization • Plan for deterring risks • Risk Modeling
2. Risk Assessment • Risk reduction plan • Risk evaluation • Risk measurement	4. Risk Monitoring • Monitoring of each significant risk • Reporting risk

Action Determination

Once the risks are identified and planning has occurred, it is necessary to prioritize the risks before the actions are taken. It is not necessary to take equal amount of response against each risk. To help prioritize risks, an organization can look to potential impact if risk is to materialize in terms of legal and regulatory, financial, or reputational damage to the organization. Risks can be avoided, reduced, transferred, or accepted depending on the organizational policies and potential of the risk; in most instances, all four are utilized. For a very serious threat, it would be advisable to avoid it. For example, an organization may decide not to provide access to organizational systems to certain individuals. To reduce the potential risk, several hardware, software, and procedural controls are implemented; this is the most important result of the risk assessment process. If the potential threat is not severe, risk can be accepted. Finally, risk transfer can be achieved using a third party, such as outsourcing certain tasks and using insurance to safeguard against potential claims.

Risk Monitoring

In a continuously evolving environment like health care IT, it is important to monitor, assess, and respond on a regular basis. Monitoring involves constant gathering of data from various points within the organization – breaches and accidents, incident alerts and reports, changes in threat levels, and counter-measures.

Reporting is not only required for making improvements in the information security process, but also required by the management, regulators, and the government. Some of the areas of reporting include summary reports for management, any type of exceptions, possible attacks that were prevented, and required reports for regulators.

CONCLUSION AND RECOMMENDATIONS

Due to the nature of personal medical information, legal, ethical, and even moral issues heighten the perception that this information is different from other electronic data. In order to produce secure information handling systems at all levels, many obstacles must be overcome. Many technical, procedural, regulatory, and practical challenges must be overcome when developing the solutions.

Because of the enormous responsibilities associated with protecting medical information, challenges and opportunities for security professionals are great. Project managers and system developers will face new situations that will have to bridge the various disciplines. There will be new opportunities for vendors to provide innovative systems to accommodate specific portions of the developing standards. Vendor alliances will be made to find solutions to the security issues facing health care organizations and help them comply with the standards, guidelines, rules, and laws.

Coordination among agencies will be imperative if standards are to be developed and widely accepted, both domestically and internationally. Small and individual health care providers to large hospital chains will need to conform to a highly set goal. Large medical center service providers will be expected to perform at high levels and meet all standards in order to demonstrate the ability to protect this information.

There are many reasons to maintain secure medical information privacy, and the privacy and security of electronic health information must be ensured as the information is collected, transmitted, maintained, and accessed electronically. Just as technical solutions are expected, stakeholders are demanding clear and legal definition of health information exchange, and many federal and state agencies are coordinating efforts to manage this challenge. Health care organizations must consider additional aspects of protecting information, including consideration of potential malicious insiders, remote access of data, firewall configurations, VPN (virtual private networking) vulnerabilities and attacks, keyloggers that steal passwords, intrusion prevention that blocks attacks, encryption options to mask the data, and adequate policies to ensure that some level of enforcement can take place if a policy is violated (Clarke et al., 2009).

Considering the current regulatory and legal environment, there are several possible steps that can be taken to reduce the risk of a lawsuit based on a data breach involving EHR information. This would include initiating training programs and information dissemination aimed at curtailing negligent behavior. Data safety is related to patient safety, and with a greater reliance on EHR treatment, it has become more important. It is important to reduce employee negligence, such as losing data through lost laptops, jump drives, and passwords left on monitors (Paray, 2011).

Health information security will continue to grow in profile as policymakers seek the widespread adoption of EHRs, especially since HITECH Act of 2009 encourages and provides incentives for the EMR adoption (Brooks and Grots, 2009). EHRs are seen as a relatively non-controversial means of improving the efficiency and effectiveness of the health care system, more so in light of recent reforms mandating increased health care access. Implemented through HHS, HIPPA is the basis of the main regulatory guidelines pertaining to EHRs and EHI with a primary focus on confidentiality. Guidelines are divided into three parts – administrative, physical and technological – and address integrity and availability, in addition to confidentiality. While no one can predict, with absolute certainty, what the future of health care will be, one can be confident in the increased role of health information security in protecting patients' health and well-being.

AUTHOR INFORMATION

Mirza B. Murtaza holds a master's degree in business from California State University and Doctorate from the University of Houston. He is an associate professor of Computer Information Systems at Middle Tennessee State University where he teaches information systems and quantitative methods at undergraduate and graduate levels. E-mail: mmurtaza@mtsu.edu

REFERENCES

1. Beeler, G. (2004). HL7 Reference Information Model, Retrieved 1/15/2012 from http://www.interopsante.org/offres/file_inline_src/412/412_P_15660_92.pdf.
2. Brooks, R. and Grotz, C. (2009). Implementation of Electronic Medical Records: How Health care Providers are Managing the Challenges of Going Digital, *Journal of Business & Economic Research*, *8*(6).
3. Caldarella, J. (2010). Privacy and Security of Personal Health Records Maintained by Online Health Services. *Albany Law Journal*, *20*(1).

4. Clarke, I., Flaherty, T., Hollis, S. and Tomallo, M. (2009) Consumer Privacy Issues associated with the Use of Electronic Health Records, *AHCMJ*, *5*(2).
5. Evans, D. C., Nichol, W. P., and Perlin, J.B. (2006). *Effect of the implementation of an enterprise-wide Electronic Health Record on productivity in the Veterans Health Administration, Health Economics, Policy and Law*, *1*(2). Cambridge University Press.
6. ISO 27001 Security (2011) ISO 27799:2008 Health informatics — Information security management in health using ISO/IEC 27002. Retrieved 1/12/2015 from http://www.iso27001security.com/html/27799.html
7. Misra, S.C., Kumar, V. and Kumar, U. (2007). A strategic modeling technique for information security risk assessment, *Information Management & Computer Security*, *15* (1). Emerald Group Publishing Limited.
8. Mukherjee, A., and McGinnis, J. (2007) E-health care: an analysis of key themes in research. *International Journal of Pharmaceutical and Health care Marketing*, *1*(4).
9. National Institutes of Health (NIH) (2006). Electronic Health Records Overview, National Center for Research Resources, National Institutes of Health.
10. Paray, P. (2011). Cost Effective Risk Management of Electronic Health information, *ISSA Journal*, Vol. 9(2). Information Systems Security Association.
11. Shaver, D. (2007) HL7 101: A Beginner's Guide. *For The Record*, *19*(1). Great Valley Publishing.

NOTES