Journal of Medicinal Plants Research Vol. 4(19), pp. 2059-2074, 4 October, 2010
Available online at http://www.academicjournals.org/JMPR
DOI: 10.5897/JMPR10.325
ISSN 1996-0875 ©2010 Academic Journals

Full Length Research Paper

Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance

Hamdan O. Alanazi[1,4], Hamid A. Jalab[1], Gazi Mahabubul Alam[3]*, B. B. Zaidan[2] and A. A. Zaidan[2]

[1]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia.
[2]Department of Electrical and Computer Engineering, Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Selangor Darul Ehsan, Malaysia.
[3]Department of Educational Management, Planning and Policy, Faculty of Education, University of Malaya, 50603 Kuala Lumpur, Malaysia.
[4]Faculty of Applied Medical Science, King Saud University, Riyadh, Kingdom of Saudi Arabia.

Accepted 7 July, 2010

Nowadays, health care is one of the most important subjects in life. In USA, 100 billion dollars will be spent on it in the next 10 years, according to experts. The Electronic Medical Record (EMR) is usually a computerized legal medical record created in an organization that delivers care, such as hospital and doctors' surgery. In the age of technology, one of the most important factors for EMR is that it secures the records for the patients, protects their rights and is responsible for the disclosure of their data. An overview of this study has presented the importance of the privacy of the EMR and the patients' rights. In addition, cryptography algorithms and security requirements have been discussed and the paper has also discussed different architecture, designs and systems that have been reported in the literature. In a nutshell, most of these systems are poor in terms of achieving the security requirements, while on the other side, most of the systems have not discussed the patients' rights and how the system can detect the persons who broadcast these records.

Key words: Electronic medical record, information security, data privacy, rights of patient and cryptography algorithms.

INTRODUCTION

Computer and information sciences and technologies are rooted in life sciences (Rao et al., 2008). Services are becoming an increasingly important element of national economies and it is crucial to appreciate the distinguishing qualities of services and resulting management implications with specific focus on healthcare services (Alam, 2009; Hashim et al., 2010; de Jager and Du Plooy, 2010). Modern medical records can benefit the scholars in contributing to their researches (Aboelsoud, 2010), and in some cases, researchers have used the medical record folders to obtain required information about patients (Bello, 2010; Bello and Itiola, 2010). Many people consider information about their health to be highly sensitive, deserving the strongest protection under the law (Bosetal, 2006; Trp e et al., 2006; Izet, 2007). Long-standing laws in many states and the age-old tradition of doctor-patient privilege have been the mainstay of privacy protection for decades (Barton, 2007). Computerized medical records pose tremendous problems to system developers (Plaisant and Rose, 1996; Phd et al., 1998; Plaisant et al., 1998; Plaisant and Mushlin, 1998). Infrastructure and privacy issues need to be resolved before physicians can even start using the records (Plaisant and Rose, 1996; Plaisant et al., 1998). Non-intrusive hardware might be required for physicians to do their work (that is, interviewing of patients) away

*Corresponding author. E-mail: gazi.alam@um.edu.my, gazimalamb@yahoo.com Tel: + 603-7967 5077. Fax: + 603-7967 5010.

from their desks and cumbersome work- stations (Plaisant et al., 1998). But all the efforts to solve such problems will only succeed if appropriate attention is also given to the design of the user interface (Plaisant and Rose, 1996; Plaisant et al., 1998). The National Research Council has established that industry spends as much as $15 billion on Information Technology (IT), an amount that is expanding by 20% per year (Anderson, 2000). Obama has pledged to invest $10 billion a year over the next five years on the effort; the price tag for such a system could be closer to $100 billion over the next 10 years, according to experts (leader). They also note that sticking to his five-year timetable could prove to be daunting. Money for the Electronic Medical Records (EMR) system would come out of the $825 billion economic stimulus package, If Obama pushes through Congress (Goldman, 2009; Marmor and Oberlander, 2009; Mearian, 2009). A certain item of information might be accessed even if stored more than 30 years. It needs to be kept unchanged all that time, and it needs to be accessible. So, both the technical integrity of the information items and the accountability of the information items need to be verifiable (Alam, 2009b). This requires specific electronic signature mechanisms and procedures that are long-lasting and long-verifiable and therefore long provable ones (Bruun-Rasmussen et al., 2003; Pharow et al., 2004, Alam et al., 2010a; Brandner et al., 2002; Pharow and Blobel, 2005). For applications like the electronic medical record, law demands methods that are secured for at least 30 years (the Legal Obligation for Medical Records) (Brandner et al., 2002; Pharow et al., 2004; Pharow and Blobel, 2005; Beyer and Hellmann, 2005; Winslade, 1982). Authentication, authorization, privacy, confidentiality, integrity and non-repudiation are terms used in security; the definition of each term explains the purpose of that term. Authentication means verifying the identity of the communicating principals to one another (Needham and Schroeder, 1978; Bellare and Rogaway, 1993), meaning that authentication approach is a verification approach (Perrig, 2001; Han et al., 2003; Becker and Meinel, 2007) while authorization is the process by which we determine whether a subject is owed to access or use an object (Nakamur and Hada, 2002). This means authorization is the granting or denial of permission to carry out a given action (Alfieri et al., 2005; Frohner and Lorentey, 2005; Jo and Kims, 2005; Lee and Winslett, 2006). Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems (Carney and Geller, 2000; Stallings, 2010). In other words, confidentiality involves protecting resources from unauthorized access and/or disclosure. Integrity involves protecting against unauthorized changes (that is, accidental or intentional) to the data (Cooper, 2009; Lee, 2009). Finally, non- repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract (McIlwraith, 2006; Harb et al., 2008; Obi and Schoenmakers, 2008).

RESEARCH QUESTIONS

This study was obtained and set up to answer the following research questions:

1. What are the rights and the privacy of patients?
2. What are the differences between law and ethics?
3. How far can you trust the computer system to secure your medical records?
4. Are the recent systems that secure your data trustworthy?
5. Can ethics stand alone to protect your rights and your privacy?
6. What is the best known algorithm that insures the security factors and is responsible for broadcasting your records?

ELECTRONIC MEDICAL RECORDS

An EMR is usually a computerized legal medical record created in an organization that delivers care, such as hospital and doctors' surgery (Dick et al., 1997). EMR tends to be a part of a local stand-alone health information system that allows storage, retrieval and manipulation of records and reduces medication errors (Sibona et al., 1899). The EMR is a longitudinal electronic record of patients' health information generated by one or more encounters in any care delivery setting (McLean, 2006; Complexity, 2007; Colesca and Zgodavova, 2008; Agbele et al., 2009). Included in this information are patients' demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports. The EMR automates and streamlines the clinician's workflow (Raghupathi and Kesh, 2007; Chaiken, 2008; Zimeras and Diomidous, 2009).

The EMR has the ability to generate a complete record of a clinical patient's encounter, as well as supporting other care-related activities directly or indirectly through interface including evidence-based decision support, quality management, and outcomes reporting (Raghupathi and Kesh, 2007; Chaiken, 2008; Colesca and Zgodavova, 2008; Agbele et al., 2009; Filker et al., 2009). An electronic record may be created for each service to a patient, such as radiology, laboratory, or pharmacy, or as a result of an administrative action (for example, creating a claim). Some clinical systems also allow electronic capture of physiological signals (for example, electrocardiography), nursing notes, physician orders, etc. (Rosenbloom et al., 2006; Tang et al., 2007; Miller and Sim, 2004; Bouchoul and Mostefai, 2009) (Figure 1).

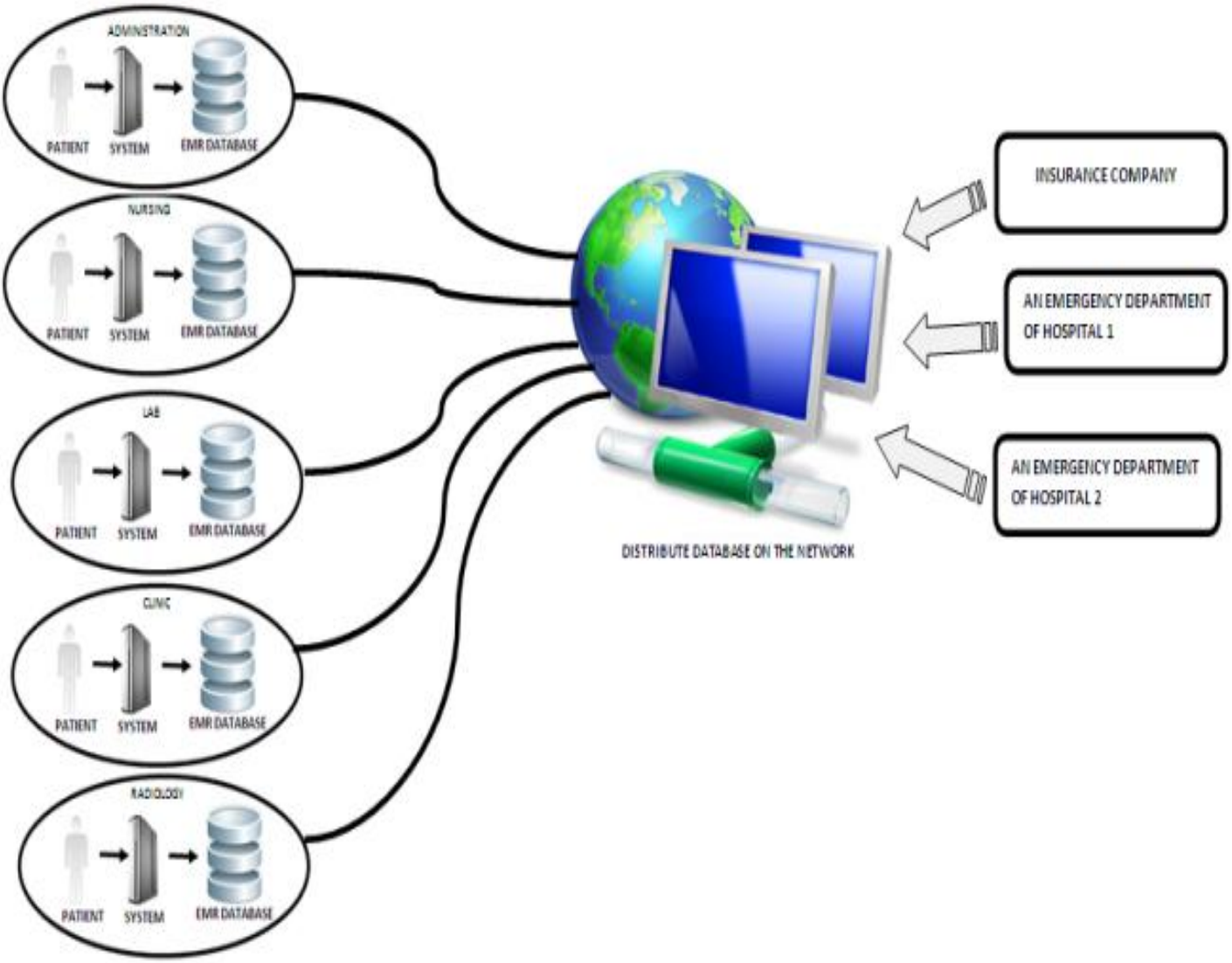

Figure 1. Electronic medical record: Distribution and accessing.

LITERATURE REVIEW

ELECTRONIC MEDICAL RECORDS THROUGH THE HISTORY

The first known medical record was developed by Hippocrates, in the fifth century B.C. He prescribed two goals:

1. A medical record should accurately reflect the course of disease.
2. A medical record should indicate the probable cause of disease (Van Bemmel et al., 1997).

These goals are still appropriate, but EMR systems can also provide additional functionality, such as interactive alerts to clinicians, interactive flow sheets, and tailored order sets, all of which can not be done with paper-based systems (McLean, 2006). The first EMRs began to appear in the 1960s. By 1965, Summerfield and Empey reported that at least 73 hospitals and clinical information projects and 28 projects for storage and retrieval of medical documents and other clinically-relevant information were underway (Dick et al., 1997). Many of today's EMRs are based on the pioneering work done in AMCs and for the Major Government Clinical Care Organizations. The Computer Stored Ambulatory Record (COSTAR), developed at Harvard, was placed in the public domain in 1975 and implemented in hundreds of sites worldwide (Bowker, 1996). Health Evaluation

through Logical Processing (HELP) was developed at Latter-Day Saints Hospital at the University of Utah (brought to market by the 3 M Corporation). HELP is notable for its pioneering decision support features (Evans et al., 1991) in the medical record (TMR) of Stead and Hammond, Duke University Medical Center (Stead and Hammond, 1988). Theresa, Walker, at Grady Memorial Hospital, Emory University, was notable for its success in encouraging direct physician data entry (Cimino, 1996). Composite Health Care System (CHCS) and the Department of Defense's (DOD) clinical care patient record system were used worldwide (Rindfleisch, 1997; Raghupathi and Tan, 2002). De-centralized Hospital Computer Program (DHCP), developed by the Veteran's Administration, was used nationwide (Hoff and Rosenheck, 1998).

Technician Data System (TDS) began in 1965 at El Camino Hospital in Mountain View, California, in conjunction with Lockheed Missiles and Space Company (Hodge, 1987; Staggers et al., 2001). These early projects had significant technical and programmatic issues, including non-standard vocabularies and system interfaces, which remain as implementation challenges today (McLean, 2006). Moreover, they lead the way and many of the ideas they pioneered (and some of the technology, such as the MUMPS language) are still used today (Morrison and Iosif, 2010; Alam et al., 2010b).

INFORMATION SECURITY

As the amount of products and services offered through the internet grows rapidly, consumers are more and more concerned about security and privacy issues (Jahangir and Begum, 2008). Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction (Everett, 2005; Stevens and Attorney, 2007; Stevens and Library of Congress Washington Dc Congressional Research, 2009). The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer (Sattarova and Kim, 2007).

Information security laws are designed to protect personally identifiable information from compromise, unauthorized access, or other situations where unauthorized persons have access or potential access to such information for unauthorized purposes (Stevens and Library of Congress Washington Dc Congressional Research, 2009). Data breach notification laws typically require covered entities to implement a breach notification policy, and include requirements for incident reporting and handling and external breach notification (Harris, 1996). Expectations of many are that efforts to enact data security legislation will continue in 2010 (Stevens and Library of Congress Washington Dc Congressional Research, 2009). In the first session of the 111th Congress, the House passed H.R. 2221, which would apply only to businesses engaged in interstate commerce and require data security programs and notification of breaches to affected consumers (Regan, 2009; Vogue et al., 2010). The Senate Judiciary Committee approved S. 139, which would apply to any agency or business engaged in interstate commerce (Stevens and Library of Congress Washington Dc Congressional Research, 2009) and S. 1490, which would apply to business entities engaged in interstate commerce and require data security programs and notification to individuals affected by a security breach. S. 1490 also includes data accuracy requirements for data brokers and requirements concerning government access to and use of commercial data (Thomas, 2009).

SECURITY REQUIREMENTS

Confidentiality

Confidential information must only be accessed, used, copied, or disclosed by users who have been authorized, and only when there is a genuine need (Pappas and Naval Postgraduate School Monterey, 2008). A confidentiality breach occurs when information or information systems have been, or may have been, accessed, used, copied, or disclosed, or by someone who was not authorized to have access to the information (Pal, 2008). For example, permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it would be a breach of confidentiality if they were not authorized to have the information. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information (Sattarova and Kim, 2007). Data confidentially refers to the attempt to keep information away from unauthorized people or systems (Smith et al., 2000; Taute, 2009). Confidentiality refers to the steps taken to ensure that confidential information is only accessed or disclosed to people who have been authorized. Even then, the information should only be accessed by those with a genuine need to view it. When businesses attempt to gain confidential information about another company, it is usually for financial gain. These businesses can use the information to sell or trade

a product for the purpose of introducing themselves into that part of the market. This will also prevent a rival company from being the “only guy on the block” with the product to offer, thus taking more of the market share (Pouloudi, 1999). The Federal Trade Commission (FTC) cited a study showing that 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential (Gellman, 2002). Confidentiality of data is not just about what the company, or government is doing. There is a whole set of information regarding people (Ardagna and Braghin, 2009).

Integrity

In information security, integrity means that data can not be modified without authorization (Sattarova and Kim, 2007). This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on (Arenas and Banâtre, 2008; Aich, 2009). There are many ways in which integrity could be violated without malicious intent (Sattarova and Kim, 2007). In the simplest case, a user on a system could miss-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity (Sattarova and Kim, 2007; Pal, 2008; Pappas and Naval Postgraduate School Monterey, 2008).

Availability

Availability means that the information, the computing systems used to process the information and the security controls used to protect the information are all available and functioning correctly when the information is needed (Sattarova and Kim, 2007; Lhotska et al., 2008; Pappas and Naval Postgraduate School Monterey, 2008). For any information system to serve its purpose, the information must be available when it is needed (Sattarova and Kim, 2007). This means that the computing systems used to store and process the information, the security controls used to protect it and the communication channels used to access it must be functioning correctly (Hwang and Syamsuddin, 2009). High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures and system upgrades. Ensuring availability also involves preventing denial-of-service attacks (Zhang and Liu, 2010).

Authenticity

Authenticity is necessary to ensure that the users or objects (like documents) are genuine (they have not been forged or fabricated) (Lhotska et al., 2008). In computing, e-Business and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are (Sattarova and Kim, 2007; Lhotska et al., 2008).

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction (Zhang and Liu, 2010). Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation (Sattarova and Kim, 2007).

RIGHTS OF PATIENT

In the rapidly changing environment of health care, many factors have influenced how health care is practiced. The rights of the patient have also been changed. Patient rights have recently become the center of national attention in the practice of medicine. Patient rights are considered as a reflection of human rights in our modern day. New elements of advanced technology medicine have added new dimensions to patient rights (Gebremariam and Hagos, 2008; Teno et al., 1993; Legemaate, 1998; Ishikawa and Konishi, 2004; Cutica et al., 2006; Fotaki, 2006; Kuzu and Ergin, 2006; Ozdemir and Er nen, 2006; Nys and Stulti, 2007; Hakan et al., 2008; Askildsen et al., 2009; Vaimaki et al., 2009). As evidenced from the prior research, web application security is one of the most important factors and future challenges, because customers fear higher risk in using the web (Haque et al., 2009).

Attention to the legal position of psychiatric patients has greatly increased during the last 25 years. As a result, among other things, the legislation with respect to involuntary admission to psychiatric hospitals has been revised in a large number of European countries (Legemaate, 1995). Under the influence of both the jurisprudence of the European Court of Human Rights in Strasbourg (Harding, 1989) and the United Nations

guidelines concerning the protection of persons with mental illness of 1991 (Anthony, 1993; Legemaate, 1998), the patient's legal position has improved. The criteria for a civil commitment have been made more stringent, the procedural guarantees have increased (Legemaate, 1995, 1998). Legal aid was introduced for patients and nowadays we pay attention to the patient's legal position during his involuntary stay in hospital. It appears that the position of mental patients has been strengthened considerably. Until the beginning of the 1970s the procedure and criteria for involuntary admission were dominated primarily by medical considerations (Legemaate, 1995, 1998).

The large international emancipation and democratization movements in the 1960s played an important role in the improvement of individual legal rights for various categories of the socially disadvantaged (Legemaate, 1998). With regard to psychiatric patients, one of the results was the new insight that the requirement of ‘due process of law' was also applicable to their involuntary admission to a hospital (Legemaate, 1995, 1998). Another view being advocated was that patients could only be restricted in exercising their civil rights in cases which serve a compelling interest of the government, and even then, only if and when there was no less-restrictive alternative available to serve that interest (Legemaate, 1995). In these requirements of proportionality and subsidiary which limitations on the legal rights of the mental patient must meet, the image of the patient as a citizen with rights emerged (Action, 2001; Legemaate, 1998). It was stipulated that the concept of citizenship with rights constitutes the core of legal protection and should be applied in constitutional states as a principle upon which the legal regulation of involuntary admission must be based. The concept of citizenship with rights entails that all citizens, no matter where they reside, whether in free 108s Legemaate-dom or in freedom-restricting institutions, must be allowed to continue to participate optimally in the law and in the application of the fundamental principles and values of justice. This means that those who are institutionalized in a psychiatric hospital must continue to enjoy their constitutional rights and other substantive civil rights and that, in so far as this is not always possible, they must be maximally accommodated in the needs for justice which are specifically inherent to the institutionalization itself. The primary aim of legal protection is to award and strengthen procedural rights and possibilities, since these enable the individual to exercise his rights and to contest decisions made with regard to him. This strengthening of individual autonomy and independence can be seen as one of the preconditions for an acceptable 'environment' as it should exist in a welfare state which is also concerned with the well-fare and well-being of its citizens, and a fortiori when involuntary admission in a psychiatric hospital is involved. As a result the discussion is no longer limited to the criteria and procedure for involuntary admission.

Nowadays it includes the patient's legal rights during his stay in hospital (hereafter referred to as the patient's internal legal position) as well. In the legislation effected in the previous century hardly any attention was paid to the internal legal position, but in the course of this century we increasingly realized that there were no good reasons for the automatic linkage of involuntary admission and incompetency. The shift from general to specific incompetence made it clear that a psychiatric disorder and/or an involuntary admission does not automatically render a patient incompetent to take decisions on certain matters. It has become necessary to develop a framework for the patient's internal legal position, addressing issues like information, consent, refusal of treatment and privacy. The discussion on the legal position of psychiatric patients usually focuses on the triangle of autonomy, beneficence and the protection of society. This triangle represents the pluralistic set of objectives of what we understand to be 'mental health': here the tension between protecting society and the protection of the individual's rights is evident. It is customary to present the notions of autonomy, beneficence and protection of society in the form of contrasts. This is quite obvious in the case of an involuntary commitment. By speaking about involuntary admission in terms of contrasts, it becomes clear that there are conflicting values and interests at stake. Generally speaking, however, we run a considerable risk of polarization and a hardening in points of view by analyzing solely in terms of contrasts. It is, for instance, not desirable to construct a black and white choice between beneficence and autonomy. It is much more a matter of degrees, a question of more or less. Wherever beneficence is overly dominant, one should aim at more autonomy. Patient, therapist and society have nothing to gain from a strong antithesis between these elements, but only by an optimal symbiosis between them. One should aim at a balance between justice and welfare. To what extent this balance is reached primarily in a legal way or by other means will depend on the conditions existing in each jurisdiction, such as legal tradition, cultural views, health care system and so on. When judging the impact of legal interventions one should always take this into account.

DATA PRIVACY

Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self (Kealy and Kelliher, 2007). Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored in digital form or otherwise (Bertino, 2005; Bertino and Extended, 2005). In some cases, these concerns refer to how data are collected, stored and associated. In other cases, the

issue is who is given access to information. Other issues include whether an individual has any ownership rights to data about them, and/or the right to view, verify and challenge that information (Walia, 2010). Various types of personal information often come under privacy concerns. For various reasons, individuals may not wish for personal information such as their religion, sexual orientation, political affiliations, or personal activities to be revealed (Sattarova and Kim, 2007). This may be to avoid discrimination, personal embarrassment, or damage to one's professional reputation (Sattarova and Kim, 2007; Walia, 2010). There is a study that shows the importance of privacy in the online environment. In a recent report to the Congress, the FTC estimated that lost online retail sales due to privacy concerns may be as much as $18 billion (Gellman, 2002).

DATA PRIVACY AND ETHICS

Ethics is a concept about moral values and rules (Kocaba and Karakose, 2009). Ethics and data privacy played an important role on data collection and data records especially for research purpose; in fact, there are differences between rules and ethics. Most of the time laws are written, approved, and then enforced by the level of government. For example, doctors have unwritten ethical rules or practices that they adhere to, just because it is the right thing to do. They have the responsibility to take care of the patients. It is ethically correct for a doctor to do his best to help the patients with their medical malady, but it is not a law that he or she has to do it. Ethics are like rules of conduct; however, ethics are not enforced by governments. In many countries there are ethics but do not reach the level of rule. The 'ethico-legal' factor comprised items relating to understanding the legislative environment and medical ethics (Pillay, 2009). For the relationship of patient and doctor, several countries have no rule to protect the patient's privacy. In other cases the insurance companies have the access to the records and they have the rights to use it. In such cases, the only thing that protects the patient's privacy is the ethics. Many researchers have used the ethics approval for the study or privacy statements such as Asadollahi et al. (2010), Kasolo and Bimenya (2010), Naseri and Ahmadi (2010) and Suwannalert et al. (2010). In addition to that, some of the researchers give a reference number for the case study such as Nkeh-Chungag and Temdie (2009), Mahmood and Mariod (2010) and Nkeh-Chungag and Bekwa (2010). However, electronic medical records should have laws instead of the ethics to ensure the right and the privacy of the patients.

SUMMARY AND CONCLUSION

Above, we have mentioned the concept of EMR, EMR from security perspective and data privacy. In fact, encryption methods are efficient way to protect data. Due to the sophistication of the attacker's methods, ways, algorithms and techniques, in addition to rapid computer hardware development, a new system designed to protect the EMR becomes an urgent need. In order to reduce perceived risk, the secure transaction mechanisms, such as information disclosure, transaction transmission, information privacy should be guaranteed and the reliability should be made known (Mondejar-Jimenez et al., 2009; Lu and Huang, 2010). Thus, software solution with proper security features may be incompatible with the current operating system or other types of software that would need to be integrated solution (Uys, 2009). Cryptography algorithms are either symmetric algorithms, which use symmetric keys (also called secret keys), or asymmetric algorithms, which use asymmetric keys (also called public and private keys). The advantages of asymmetric cryptography over symmetric cryptography are that symmetric cryptography provides integrity, authenticity and non-repudiation in addition to confidentiality. The literature reported many design, protocols, architecture and systems to secure the EMR. However, these approaches have many weaknesses for instance, an approach that provides confidentiality, integrity but non-repudiation is not guarantee.

Rivest, Shamir and Adleman (RSA) and Elliptic Curve Cryptosystems (ECC) were considered as the widest PKI algorithms. In the literature, they reported many weaknesses on RSA (Kuz and Rauch, 2001; Freeman, 1995; Matsui et al., 2000; Karu and Loikkanen, 2001; Morogan, 2005). They stated that RSA is slow (Kurosawa et al., 1994) and insecure if the same message is encrypted to several receivers. To completely break RSA one needs to find the prime factors. In practice, RSA has proved to be quite slow, especially for key generation algorithm. RSA also requires longer keys in order to be secure compared to some other cryptosystems like ECC (Karu and Loikkanen, 2001). In the middle of the 90s, ECC has appeared; it is faster than RSA (Chung et al., 2007; Vincent et al., 2010), has-160 has 6X smaller key-size than RSA-1024 and can generate a signature 12 times faster than RSA (Balitanas et al., 2009). It is faster and occupies less memory space than an equivalent RSA system (Kapoor and Abraham, 2008), generates asymmetry keys pair faster than RSA (Rui et al., 2009), is more efficient than the ubiquitous RSA based schemes because it utilizes smaller key sizes for equivalent security (Sriram et al., 2010). Security-wise ECC is stronger than RSA (Kute and Paradhi, 2009). In 2009, a new standard has been approved for PKI called NTRU cryptosystem. Preliminary experimental results show the advantages of NTRU over RSA, such as, at the similar security level, the key size of NTRU is less than a quarter of that of RSA, and the speed of NTRU is much faster than that of RSA; the key generation is more than 200 times faster (Shen et al., 2009). NTRU can execute 2000

Table 1. Literature survey.

No	Goal	Drop-back	Year	Citation
(Ferreira et al., 2004)	They present guarantee that when there is the need to access patient reports, whether now or in 20 years' time, those are still stable and valid to be integrated within the electronic patient records.	According to (Bonet et al., 1997; Kurosawa et al., 1995; Lei et al., 2005; Saxena, 2006; Thapen, 2006; Guan, 2007; Tartary, 2007; Maitra and Sarkar, 2008a, 2008b; Schridde et al., 2009) RSA is no more secure.	2004	15
(Brandner et al., 2002)	They provide an electronic signature using Public Key Infrastructure in Hospitals. They also mentioned about the signature law and how it has to be integrated in electronic patient records and provided with standardized interfaces to certification services. The proposed PKI is based on the German Signature Law.		2002	37
(Smith, 1995)	They pretend that RSA Digital Signature Technology can establish the authenticity of images to at least the level of confidence required for interbank electronic transfer of funds.		1995	16
(Janbandhu and Siyal, 2001)	They have introduced the notion of biometric signature, the new approach has integrated biometrics with PKI using biometric based on digital signature generation. They also suggest two schemes for biometric signature using two digital signature algorithms, RSA and Digital Signature Algorithm. The new schemes (based on iris recognition) is measured and compared with the help of JAVA implementation for both approaches.		2001	33
(Epstein et al., 1998)	They give an overview of new security concerns, new legislation mandating secure medical records and solutions providing security and they present that RSA as a digital signature algorithm.		1998	25

Table 1 Contd.

(Bos et al., 2004)	They have mentioned that the majority of security services nowadays are based on public key Infrastructure using asymmetric cryptographic algorithms, for example, the well-known RSA. Page 435.		2004	5
(Gobi and Vivekanandan, 2009)	They suggest an implementation of a digital envelope that combines the hashing algorithm of MD5, the symmetric key algorithm of AES and the asymmetric key algorithm of Hyper Elliptic Curve Cryptography (HECC).	Due to the hardware and memory requirements, this implementation is very sound costly. In the same time the author has not carried out Certifying Authority (CA) in place. All the certificates that are used in those systems are considered to be trusted.	2009	No citation
(McGuire and Fisher, 2008)	This article discusses characteristics of genetic/genomic test information, including predictive capability, immutability, and uniqueness, which should be considered when developing policies about information protection.	There some points are required farther improvements. In additional the technical perspective has not stated. As well, the protection of the electronic patient record has not clearly mentioned.	2002	9
(Anderson, 2000)	They identify a number of important health information policy issues. They also present that the main threats to privacy and confidentiality arise from within the institutions that provide patient care as well as institutions that have access to patient data for secondary purposes.	He has identified the importance the Security of the distributed electronic patient record in a good way. However the security requirements were not clear and the reference to the capable solution was absent	2000	34
(De Meyer and Lundgren, 1998)	They give an overview of requirements and constraints when communicating electronic medical record information. They also mentioned that the most challenging security aspect of electronic health care record communication is the decision process, which precedes the actual transmission. It is there that problems persist which require a further convergence between the legal aspects and the technical solutions.	They have presented a good work. Nevertheless, They did not mention which algorithm that they have used. The performance is very important consider in this state. The security requirements are mentioned but their implementations were not clear.	1998	15

Table 1. Contd.

(Rind et al., 1997)	They describe an explicit protocol that would make it possible to electronically identify patients and providers, secure permission for release of records, and track information that is transmitted. It is hoped that other, similar efforts now underway will be able to use and build on this model. Comment on this proposal is invited from all parties with an interest in confidentiality. The system will be used only with "scrubbed" data—data from which all identifiers have been removed—until it is generally agreed that the confidentiality methods proposed appropriate and sufficient.	There are some points need to be improved in this paper, no clearly indicated procedure is presented for transmission EMR among institutions. Second, they did not mention clearly how they will protect the confidentiality of the patients. Third, it is not clear whether there is securing for EMR through the transmission. Fourth, nothing has been mentioned who may have access to the record in the recipient institution after the emergency has passed. Finally, the rule has not been addressed any of the issues related to the electronic transmission of patient records between different entities that belong with the same corporate network.	1997	113
(O'Brien and Yasnoff, 1999)	This study to assess the employment and status of privacy, confidentiality, security and fair information practices in electronic information systems of U.S state health agencies. They also mentioned that preservation of privacy need not necessitate withholding information completely	They have covered under the Privacy and Confidentiality of Computerized Data part. Some of the security requirements such as Confidentiality, integrity and authenticate. However, they did not cover very important factor Non-repudiation. In addition, it is not clearly mentioned which PKI algorithm has been used.	1999	20

times faster than other public key cryptosystems. While it takes up only 1/50 of the memory space, others take more than that (Bu and Zhang, 2009). The implementation with product form polynomials gives a speed of more than 200, 000 encryptions per second or 41.8 M-Byte/s. Overall, NTRU key generation over RSA is more than 200 times faster (Shen et al., 2009) (Table 1).

In the approaches that have been mentioned in the work:

1. Symmetric and asymmetric cryptography have been adapted to secure EMR: however, a system that guarantees confidentiality, integrity, authenticity, availability and non-repudiation has not appeared in the literature.
2. RSA and ECC are very slow and required long processing, extra memory, extra cost and long key.
3. For applications like the electronic patient record, law demands methods that are secured for at least 30 years (the legal obligation for medical records). The availability of RSA and ECC attackers made using these algorithms not suitable for such applications.
4. In the cases of any disclosure to the patient's A record, the patient's legal state is not concerned, while the approaches pay the attention to data privacy not the patients' rights.
5. Symmetric cryptography is not an available choice because it can not provide confidentiality repudiation (Tables 2 and 3 and Figures 2 and 3).

As it has been mentioned in the work, the EMR has become a very important matter in life. In addition, security, privacy of the patient, access gain control and the distribution of EMR are very hot subjects to be researched. The patients' rights

Table 2. The description of the life cycle of EMR.

No.	Description
1	Doctor will treat the patient and the patient will describe his condition
2	In the medical profession there should be ethics for doctors to follow (there is no punishment for not following).
3	Doctor knows that no law governing the relationship with the patient and it will be responsible when abused his powers to act in.
4	The powers of the doctor access to medical records relating to the patient and analyzes the results of previous drugs used by patients and medical history at the same time will add the new results of the visits
5	The patient has powers of access to his medical records.
6	The law can protect the rights of the patient.
7	The law regulates the protection of the patient and the powers of access to medical records relating to the accounting and responsible for misuse.
8	Will analyze and prepare the law to be applied.
9	To access the security requirements must be analyzed Law.
10	To implement the security requirements on the medical records of patients must be used in computer science.
11	Computer Science will apply the medical records of patients and meet the requirements of security and will also resolve any technical problems for the future.

Table 3. Critical review.

Paper	Security Objectives					Algorithms						Protection of patient's privacy
	Conf.	Non-R	Auth.	Inti.	D.I	Asymm.			Symm.			
						RSA	ECC	NTRU	AES	DES	3DES	
(Blobel 2000)	X	✓	✓	✓	X	X	X	X	X	X	X	X
(Gritzalis 2007)	✓	✓	✓	✓	X	✓ X	X	X	X	X	X	X
(Espinosa 1998)	✓	X	X	X	X	X	X	X	X	X	X	X
(Bos 1996)	✓	✓	✓	✓	X	✓	X	X	X	X	X	X
(Blobel and Roger-France 2001)	✓	✓	✓	✓	X	✓	X	X	X	X	X	X
(Pharow and Blobel 2005)	✓	✓	✓	✓	X	✓	X	X	X	X	X	X
(Kluge 2007)	X	X	X	X	X	X	X	X	X	X	X	X
(Ahmad 2009)	✓	X	✓	✓	X	X	X	X	X	X	X	X
-)	✓	X	✓	✓	X	X	X	X	X	X	X	X

need to be secured and the law should act on it. These days, technology helps in different ways to make life easier and safer. In the medical side, information security assists to protect the patient's privacy, while on the aspect of law, it plays a more important role in defending the patient if his or her data are been illegally used. The paper has discussed the factors of security, encryptions algorithms, patients' rights, ethics and the EMR systems that have appeared in the literature. In addition, the author has supported his findings by many literatures and depicted the integrity,

Table 2. Contd.

(Takeda et al., 2004)	✓	X	✓	✓	X	X	X	X	X	X	X	X
(Hu et al., 2009)	✓	✓	✓	✓	X	X	X	X	X	X	X	X
(Kalra and Talmon, 2009)	✓	✓	✓	✓	X	X	X	X	X	X	X	X
(Sucurovic, 2007)	✓	X	✓	X	X	✓	X	X	✓	X	X	X
(Bonacina et al., 2010)	✓	✓	✓	✓	X	✓	X	X	✓	X	X	X
(Smith and Eloff, 1999)	✓	X	✓	✓	X	✓	X	X	X	✓	X	X
(Van der Haak al., 2003)	✓	X	✓	✓	X	✓	X	X	X	✓	X	X
(Ferreira et al., 2004)	X	X	X	✓	X	X	X	X	X	X	X	X
(Brandner et al., 2002)	✓	✓	✓	✓	X	✓	X	X	X	X	X	✓
(Smith, 1995)	✓	✓	✓	✓	X	X	X	X	X	X	X	X
(Janbandhu and Siyal, 2001)	X	X	✓	X	X	✓	X	X	X	X	X	X
(Epstein et al., 1998)	X	X	✓	✓	X	✓	X	X	X	X	X	X
(Gobi and Vivekanandan, 2009)	✓	✓	✓	✓	✓	X	✓	X	✓	X	X	✓
(McGuire et al., 2008)	X	X	X	X	X	X	X	X	X	X	X	X
(Anderson, 2000)	X	X	X	X	X	X	X	X	X	X	X	X
(de Meyer et al., 1998)	✓	✓	✓	✓	X	X	X	X	X	X	X	X
(Rind et al., 1997)	✓	X	✓	✓	X	X	X	X	X	X	X	X
(O'Brien and Yasnoff, 1999)	✓	X	✓	✓	X	X	X	X	X	X	X	X

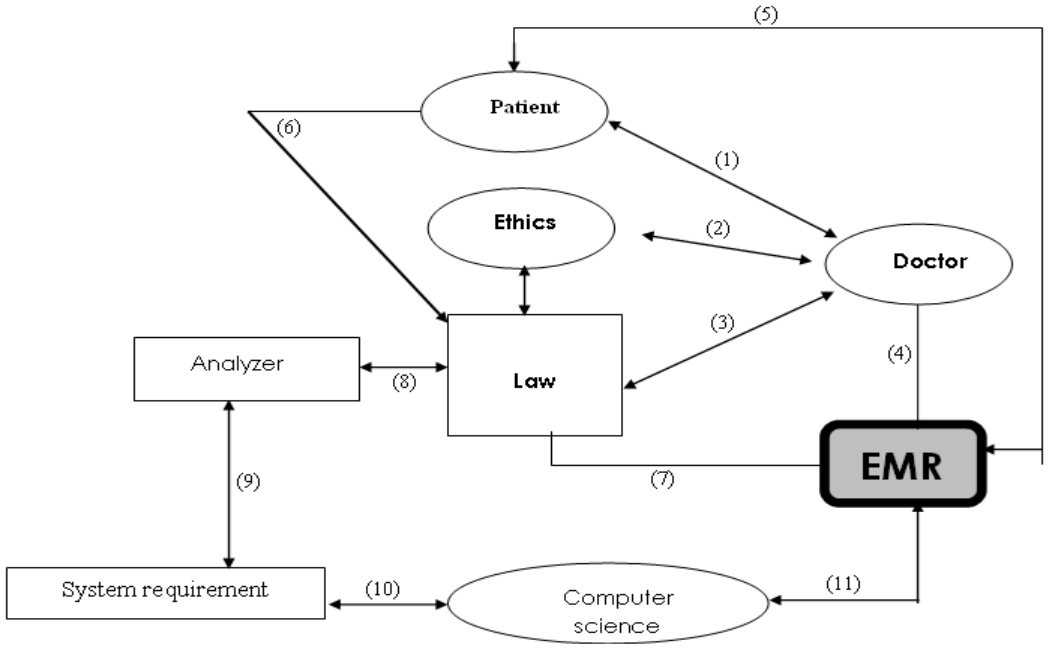

Figure 2. The life cycle of EMR.

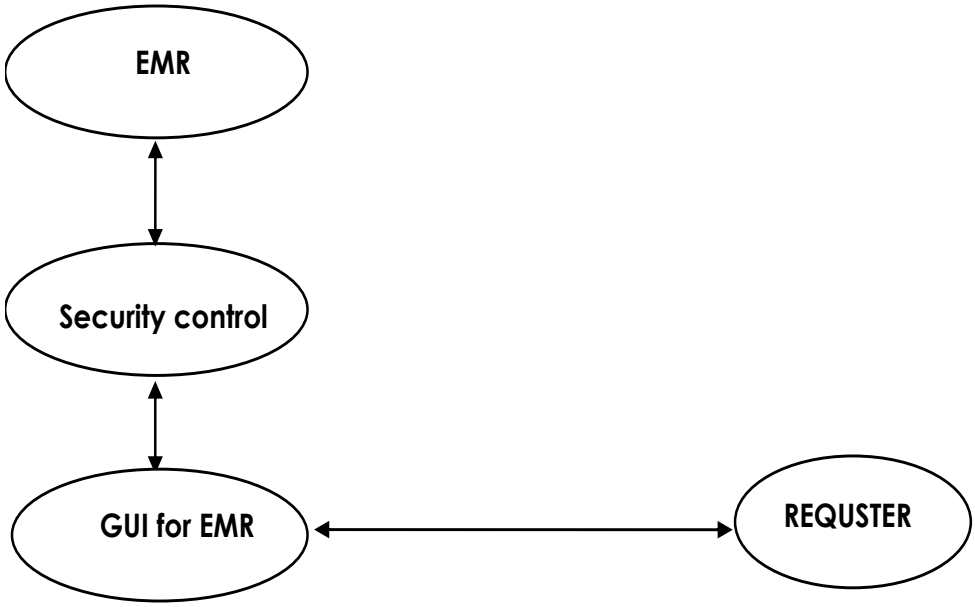

Figure 3. Operations to access the EMR.

authenticity, availability and non-weaknesses of the recent systems to secure the transmission over unsecured communications, for better medical governance.

ACKNOWLEDGEMENTS

This research has been funded in part by the University of Malaya, King Saud University and Multimedia University. The author would like to acknowledge all workers involved in this project who had given their support in many ways

Abbreviations: EMR, Electronic medical record; **EHR,** electronic health record; **Conf,** confidentiality; **Non-R,** non-repudiation; Auth, authenticity; **Inti,** integrity; **D.E,** digital envelop; **Asymm,** asymmetric; Symm, symmetric; **IT,** information technology; **AMCs,** American medical clinics; **COSTAR,** the computer stored ambulatory record; **HELP,** health evaluation through logical processing; **TMR,** the medical record**; CHCS,** composite health care system**; DOD,** partment of defense's**; DHCP,** de-centralized hospital computer program; **TDS,** technician data system; **RSA,** rivest, shamir and adleman; **ECC,** elliptic curve cryptography; **PKI,** public key infrastructure.

REFERENCES

Alam GM (2009a). The role of science and technology education at network age population for sustainable development of Bangladesh through human resource advancement. Sci. Res. Essays, 4(11): 1260-1270.

Alam GM (2009b). Can governance and regulatory control ensure private higher education as business or public goods in Bangladesh? Afr. J. Bus. Manage., 3(12): 890-906.

Alam GM, Oke OK, Orimogunje T (2010a). Volumetric analysis and chemistry students performance: combined influence of study habit, physiological and psychological factors, Sci. Res. Essays, 5(11): 1325-1332.

Alam GM, Oloruntegbe KO, Oluwatelure TA, Alake, ME, Ayeni EA (2010). Is 3D just an addition of 1 to 2 or is it more enhancing than 2D visualizations? Sci. Res. Essays, 5(12): 1536 - 1539

Aboelsoud NH (2010). "Herbal medicine in ancient Egypt." J. Med. Plants. Res., 4(2): 082-086.

Action C (2001). "Ethical aspects deinstitutionalisation in mental health care."

Agbele K, Nyongesa H (2009). "Search in Medwell." J. Mobile. Comm. 3(4): 17-22.

Ahmad N (2009). "Restrictions on cryptography in india-a case study of encryption and privacy." Compu. Law Security Rev., 25(2): 173-180.

Aich D (2009). "Secure Query Processing by Blocking SQL injection." Alfieri R, Cecchini R (2005). "From gridmap-file to VOMS: Manag. Syst., 21(4): 549-558.

Anderson JG (2000). "Security of the distributed electronic patient record: a case-based approach to identifying policy issues." Inter. J. Med. Infor., 60(2): 111-118.

Anthony WA (1993). "Recovery from mental illness: The guiding vision of the mental health service system in the 1990s." Psychosocial. Rehabilitation J. 16: 11-11.

Ardagna, Braghin CAC (2009). "NET PRIVACY."

Arenas A, Banâtre JP (2008). "Developing Secure Chemical Programs with Aspects."

Asadollahi K, Abassi N (2010). "Investigation of the effects of Prosopis farcta plant extract on Rat's aorta." J. Med. Plants. Res., 4(2): 142-147.

Askildsen JE, Holm s TH (2009). "Prioritization and patients' rights: Analysing the effect of a reform in the Norwegian hospital sector." Social Science & Medicine.

Balitanas MO, Robles RJ (2009). Crossed Crypto-Scheme in WPA PSK Mode, IEEE.

Barton BH (2007). "Do Judges Systematically Favor the Interests of the Legal Profession." Ala. L. Rev., 59: 453.

Becker T, Meinel C (2007). "Security in Telemedicine–Certificates and Digital Identity Cards."

Bellare M, Rogaway P (1993). Entity authentication and key distribution, Springer.

Bello SI (2010). "Challenges of DOTS implementation strategy in the treatment of tuberculosis in a tertiary health institution, Ilorin, Nigeria." Afr. J. Pharmacy. Pharmacol., 4(4): 158-164.
Bello SI, Itiola OA (2010). "Drug adherence amongst tuberculosis patients in the University of Ilorin Teaching Hospital, Ilorin, Nigeria." Afr. J. Pharm. Pharmacol., 4(3): 109-114.
Bertino E, "Overview of Information Security."
Bertino E, Extended R (2005). "Data Privacy."
Beyer A, Hellmann S. "Criteria for success of identification, authentication and signing methods based on asymmetric cryptographic algorithms (EKIAS)."
Blobel B (2000). "Advanced tool kits for EPR security." Inter. J. Med. Inform., 60(2): 169-175.
Blobel B, Roger-France F (2001). "A systematic approach for analysis and design of secure health information systems." Inter. J. Med. Informatics., 62(1): 51-78.
Bonacina S, Marceglia S, Bertoldi M, Pinciroli F (2010). "Modelling, designing, and implementing a family-based health record prototype." Compu. Biol. Med. 40(6): 580-590.
Bonet ML, Pitassi T, "No Feasible Interpolation for TC."
Bos JJ (1996). "Digital signatures and the electronic health records: providing legal and security guarantees." Inter. J. Bio-med. Compu., 42(1-2): 157-163.
Bos L, Laxminarayan S,Marsh A (2004). Medical and care compunetics 1, Ios Pr Inc.
Bosetal L (2006). "BioHealth-The Need for Security and Identity Management Standards in eHealth." Med. Care Compunetics 3: 327.
Bouchoul FM, Mostefai (2009). "Agent-services and mobile agents for an integrated HCIS." Int. J. Compu. Integr. Manuf., 22(5): 458-471.
Bowker GC (1996). "The history of information infrastructures: The case of the international classification of diseases." Info.. Proc.. Manage., 32(1): 49-61.
Brandner R, Van der Haak M (2002). "Electronic Signature of Medical Documents--Integration and Evaluation of a Public Key Infrastructure in Hospitals." Methods of Information in Medicine-Methodik der Information in der Medizin, 41(4): 321-330.
Bruun-Rasmussen M, Kaae T, Tynan L, Chronakie CE (2003). "The impact of EHR and digital electrocardiograms." The new navigators: from professionals to patients: proceedings of MIE2003
Bu SY, Zhang H (2009). Research on the Method of Choosing Parameters for NTRU, IEEE.
Carney PA, Geller BM (2000). "Current medicolegal and confidentiality issues in large, multicenter research programs." Am. J. Epidemiol., 152(4): 371.
Chaiken BP (2008). "Healthcare IT solutions." The Business of Healthcare. pp. 127–29.
Chung YF, Huang KH, Lai F, Chen TS (2007). "ID-based digita signature scheme on the elliptic curve cryptosystem." Compu. Stand. Interfaces 29(6): 601-604.
Cimino JJ (1996). "Review paper: coding systems in health care." Meth. Inf. Med., 35(4-5): 273-284.
Colesca SE, Zgodavova K (2008). "Transforming Healthcare Quality through Information Tehnology." Economia. Seria Manage., 11(1): 21-39.
Complexity H (2007). "Electronic Medical Records: Healthcare
Complexity, Lack of Definition And Communication Creates Confusion."
Cooper MH (2009). Information security training: what will you communicate?, ACM.
Cutica I, Bucciarelli M, Bara BG (2006). "Neuropragmatics: extralinguistic pragmatic ability is better preserved in left-hemisphere-damaged patients than in right-hemisphere-damaged patients." Brain Lang. 98(1): 12-25.
de Jager JW, du Plooy AT (2010). "Delivering quality service to in-and out-patients in a South African public hospital." Afr. J. Bus. Manage., 4(2): 133-139.
de Meyer F, Lundgren PA (1998). "Determination of user requirements for the secure communication of electronic medical record information." Inter. J. Med. Inform., 49(1): 125-130.
Dick R S, Steen EB, Detmer DE (1997). The computer-based patient record: an essential technology for health care, Natl Academy Pr.
Encryption EG, "Public-Key Cryptography."Class. Introduc. Cryptogr., 229-251.
Epstein MA, Pasieka MS (1998). "Security for the digital information age of medicine: issues, applications, and implementation." J. Digital. Imaging. 11(1): 33-44.
Espinosa AL (1998). "Availability of health data: requirements and solutions." Inter. J. Med. Inform., 49(1): 97-104.
Evans RS, Pestotnik SL, Classen DC, Bass SB, Menlove RL, Gardner RM, Burke JP (1991). Development of a computerized adverse drug event monitor, American Medical Informatics Association.
Ferreira A, Cruz-Correia R, Antunes L, Palhares E, Marques P, Costa P, Costa-Pereira A (2004). Integrity for electronic patient record reports, IEEE Computer Society.
Filker PJ, Muckey EJ, Kelner SM, Kodish-Stav J (2009). "Taking a Quality Assurance Program From Paper to Electronic Health Records: One Dental School's Experience." J. Dental Edu. 73(9): 1095.
Fotaki M (2006). "Users' perceptions of health care reforms: Quality of care and patient rights in four regions in the Russian Federation." Soc. Sci. Med., 63(6): 1637-1647.
Freeman W (1995). "A novel chained-block byte-vector cipher intended for software implementation." report-university of york department of computer science ycs.
Frohner A, Lorentey K (2005). "From gridmap-file to VOMS: managing authorization in a Grid environment." Future Gene. Compu. Syst., 21: 549-558.
Gebremariam T, Hagos M (2008)."Situation Analysis of Medico-Legal Issues in Asmara, Eritrea, in " J. Eritrean. Med. Assoc., 4(1): 31.
Gellman R (2002). Privacy, Consumers, and Costs.pp235
Gobi M, Vivekanandan K (2009). "A New Digital Envelope Approach for Secure Electronic Medical Records." IJCSNS 9(1): 1.
Goldman HH (2009). "President Obama and Mental Health Policy–the Audacity to Hope." J. Mental. Health., 18(3): 193-197.
Gritzalis DLD (2007). "Long-term verifiability of the electronic healthcare records' authenticity." Inter. J. Med. Inform., 76: 5/6.
Guan DJ (2007). "Introduction to Security Proof of Cryptosystems."
Hakan M, Ozgur CI (2008). "Midwives and nurses awareness of patients' rights." Midwifery.
Han CC, Cheng HL, Lin CL, Fan KC (2003). "Personal authentication using palm-print features* 1." Pat. Recognit., 36(2): 371-381.
Haque A, Tarofder AK, Rahman S, Raquib MA (2009). "Electronic transaction of internet banking and its perception of Malaysian online customers." Afr. J. Bus. Manage 3(6): 248-259.
Harb H, Farahat H, Ezz M (2008). SecureSMSPay: Secure SMS Mobile Payment model.
Hashim F, Alam GM, Siraj S (2010). Information and communication technology for participatory based decision-making-E-management
for administrative efficiency in Higher Education. Inter. J. Phys. Sci., 5(4): 383-392.
Harding TW (1989). "The application of the European Convention of Human Rights to the field of psychiatry." Inter. J. Law. Psychiatry., 12(4): 245-262.
Harris RE (1996). "Need to Know versus the Right to Know: Privacy of Patient Medical Data in an Information-Based Society, The." Suffolk UL Rev. 30: 1183.
Hodge MH (1987). History of the TDS medical information system, ACM.
Hoff RA, Rosenheck RA (1998). "The quality of VA mental health services." Admin. Pol. Mental Health Mental Health Serv. Res., 26(1): 45-56.
Hu J, Chen HH (2009). "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations." Compu. Stand. Interfaces.
Hwang J, Syamsuddin I (2009). Information Security Policy Decision Making: An Analytic Hierarchy Process Approach, IEEE.
Ishikawa K, Konishi N (2004). "A clinical management system for patient participatory health care support:: Assuring the patients' rights and confirming operation of clinical treatment and hospital administration." Inter. J. Med. Inform., 73(3): 243-249.
Izet Masic HP (2007). Requirements for Security and Privacy, Pro Universitate.
Jahangir N, Begum N (2008). "The role of perceived usefulness, perceived ease of use, security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking."

Afr. J. Bus. Manage. 2(1): 032-040.
Janbandhu PK, Siyal MY (2001). "Novel biometric digital signatures for Internet-based applications." Info. Manage. Compu. Secur., 9(5): 205-212.
Janczewski L, Shi X (2002). "Development of information security baselines for healthcare information systems in New Zealand." Compu. Secur.,, 21(2): 172-192.
Jo SM, Kim KT (2005). Access Authorization Policy for XML Document Security, Springer.
Julià-Barcel R, Vinje T. "Towards a european framework for digital signatures and encryption": The European commission takes a step forward for confidential and secure electronic communications." Compu. Law Secur. Report 14(2): 79-86.
Kalra HLD, Talmon AHJ (2009). "Inter-organizational Future Proof Ehr Systems A Review Of the Security and Privacy Related Issues." Int. J. Med. Inform. 78: 3.
Kapoor V, Abraham VS (2008). "Elliptic curve cryptography." Ubiquity 9(20): 1.
Karu P, Loikkanen J (2001). "Practical comparison of fast public-key cryptosystems." Manuscript.
Kasolo JN, Bimenya GS (2010). "Phytochemicals and uses of Moringa oleifera leaves in Ugandan rural communities." J. Med.Plants. Res., 9: 753-757.
Kealy A, Kelliher F (2007). An Exploratory Investigation into Internet Users' Perception Regarding the Data Privacy Policies of Virtual Companies Operating in Ireland, Academic Conferences Limited.
Kluge EHW (2007). "Secure e-health: managing risks to patient health data." Inter. J. Md. Inform.76(5-6): 402-406.
Kocaba I, Karaköse T (2009). "Ethics in school administration." Afr.J. Bus. Manage. 3(4): 126-130.
Kurosawa K, Okada K."Low exponent attack against elliptic curve RSA." Advances in Cryptology—ASIACRYPT'94: 376-383.
Kurosawa K, Okada K."y Dept. of Electrical & Electronic Eng. Tokyo Institute of Technology 2 {12 {1 O-okayama, Meguro-ku, Tokyo 152, JAPAN (kkurosaw@ ss. titech. ac. jp) z Dept. of Computer Science."
Kute VB, Paradhi PR (2009). "A SOFTWARE COMPARISON OF RSA AND ECC." Int. J. Compu. Sci. Appl. 2:1.
Kuz I, Rauch F. "COMP9243—Week 8 (09s1)."
Kuzu N, Ergin A (2006). "Patients' awareness of their rights in a developing country." Public health 120(4): 290-296.
Leader S,"Scoping Environmental e-Health: Understanding the Environmental Benefits and Costs of using ICT to Facilitate Healthcare (e-Health)."
Lee AJ, Winslett M (2006). Traust: a trust negotiation-based authorization service for open systems, ACM.
Lee HJ (2009). "A review of IPTV threats based on the value chain." KSII Transactions on the Internet and Systems **3**(2): 163-77.
Legemaate J (1995). "Involuntary Admission to the Psychiatric Hospital:
Recent European Developments." Eur. J. Health L,**2**: 15.
Legemaate J (1998). "Legal protection in psychiatry: balancing the rights and needs of patients and society." Eur. Psychiatry 13: 107-112.
Lei F, Chen W, Chen K (2005)."Improvement of Adaptive Threshold RSA." EC2ND 2005: 157-164.
Lhotska L, Prague C, Aubrecht P (2008). "Deliverable D09 Security of the Multi Agent System." Agent System."
Lu CT, Huang SY (2010). "An empirical study of on-line tax filing acceptance model: Integrating TAM and TPB." Afr. J. Bus. Manage. 4(5): 800-810.
Mahmood AA, Mariod AA (2010). "Anti-ulcerogenic activity of Gynura procumbens leaf extract against experimentally-induced gastric lesions in rats." J. Med.Plants.Res,4(8): 685-691.
Maitra S, Sarkar S (2008). "Revisiting Wiener's attack–new weak keys in RSA." Information Security Springer Berlin / Heidelberg: 228-243.
Maitra S, Sarkar S (2008). Revisiting Wiener's Attack–NewWeakKeysinRSA, Springer-Verlag New York Inc.
Marmor T, O berlander J (2009). "The Obama administration's options for health care cost control: hope versus reality." Ann. Int. Med., 50(7):485.
Matsui T, Kobayashi M (2000). Method, apparatus, system and information storage medium for wireless communication, Google Patents.
McGuire AL, Fisher R (2008). "Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider." Genet. Med.,10(7): 495.
McIlwraith A (2006). Information security and employee behaviour: how to reduce risk through employee education, training and awareness, Gower Pub Co.
McLean V (2006). "Electronic Health Records Overview."
Mearian L (2009). Obama's national health records system will be costly, daunting But an electronic health records system could save the nation $300B a year. computerworld.
Miller RH, Sim I (2004). "Physicians' use of electronic medical records: barriers and solutions." Health Affairs 23(2): 116.
Mondéjar-Jiménez JA, Mondéjar-Jiménez J (2009). "E-commerce and legal protection for consumers: Spanish analysis." Afr. J. Bus. Manage. 3(9): 426-432.
Morogan MC (2005). "Efficient Key Management Scheme for Mobile Ad Hoc Network."
Morrison C, Iosif A (2010). "Report on existing open-source electronic medical records."
Nakamur Y, Hada S (2002). "Towards the integration of Web services security on enterprise environments." saint-w: 166.
Naseri M, Ahmadi A (2010). "A double blind, placebo-controlled, crossover study on the effect of MS14, an herbal-marine drug, on quality of life in patients with multiple sclerosis." J. Med. Plants. Res. 3(4): 271-275.
Needham RM, Schroeder MD (1978). "Using encryption for authentication in large networks of computers." Communications of the ACM 21(12): 999.
Nkeh-Chungag BN, Temdie JR (2009). "Analgesic, anti-inflammatory and antiulcer properties of the extract of Uapaca guineensis (Euphorbiaceae)." J. Med. Plants. Res**. 3**(9): 635-640.
Nkeh-Chungag NB, Bekwa PCM (2010). "Analgesic and anti-inflammatory properties of Oxyanthus unilocularis." J. Med. Plants. Res., 4(10): 932-939.
Nys H, Stulti L (2007). "Patient rights in EU Member States after the ratification of the Convention on Human Rights and Biomedicine." Health Policy 83(2-3): 223-235.
O'Brien DG, Yasnoff WA (1999). "Privacy, confidentiality, and security in information systems of state health agencies." Am. J. Prev. Med., 16(4): 351-358.
Obi CO, Schoenmakers LAM (2008). "Security Issues in Helper Data Systems."
Ozdemir MH, Ergnen AT (2006). "The approach taken by the physicians working at educational hospitals in Izmir towards patient rights." Patient Educ. Couns., 61(1): 87-91.
Pal RK (2008). Design and Implementation of Secure File System, Indian Institute of Technology.
Pappas JA, CA Naval Postgraduate School Monterey (2008). A Revitalized Information Assurance Training Approach and Information Assurance Best Practice Rule Set, Naval Post Graduate School Monterey Ca.
Perrig A (2001). The BiBa one-time signature and broadcast authentication protocol, ACM.
Pharow P, Blobel B (2005). "Electronic signatures for long-lasting storage purposes in electronic archives."Int. J. Med. Inform.,74(2-4): 279-287.
Pharow P, Blobel B, Press IOS, Bos L, Laxminarayan S, Marsh A, Buchkapitel NPR (2004). "Security infrastructure services for electronic archives and electronic health records." Med. Care compunetics 1: 434.
Phd CP, Plaisant C, Mushlin R, Snyder A, Li J, Heller D, Shneiderman B, Colorado KP (1998). "LifeLines: Using Visualization to Enhance Navigation and Analysis of Patient Records."
Pillay R (2009). "Perceived competencies of nurse managers: A comparative analysis of the public and private sectors in South Africa." Afr. J. Bus. Manage. 3(9): 495-503.
Plaisant C, Heller D, Li J, Shneiderman B, Mushlin R, Karat J (1998a). Visualizing medical records with LifeLines, ACM.
Plaisant C, Heller D, Li J, Shneiderman B, Mushlin R, Karat J (1998a). Visualizing medical records with LifeLines, ACM.
Plaisant C, Mushlin R (1998). LifeLines: using visualization to enhance navigation and analysis of patient records, Am. Med. Inform. Assoc.,

Plaisant C, Rose A (1996). Exploring LifeLines to visualize patient records, Citeseer.
Pouloudi A (1999). "Information technology for collaborative advantage in healthcare revisited." Info, Manage., 35(6): 345-356.
Raghupathi W, Kesh S (2007). "Interoperable Electronic Health Records Design: Towards a Service-Oriented Architecture." e-Service.J, 5(3): 39-57.
Raghupathi W, Tan J (2002). "Strategic IT applications in health care." Communications of the ACM 45(12): 61.
Rao VS, Das SK, Rao VJ,Srinubabu G (2008). "Recent developments in life sciences research: Role of bioinformatics." Afr. J. Biotech., 7(5): 495-503.
Regan PM (2009). "Security Breach Notification Six Years Later: Federal Security Breach Notifications: Politics and Approaches." Berkeley Tech. LJ 24: 1103-1239.
Rind DM, Kohane IS, Szolovits P, Safran C,Chueh HC,Barnett G. (1997). "Maintaining the confidentiality of medical records shared over the Internet and the World Wide Web." Ann. Intern. Med. 127(2): 138.
Rindfleisch TC (1997). "Privacy, information technology, and health care." Commun. ACM, 40(8): 92-100.
Rosenbloom ST, Miller RA, Johnson KB, Elkin PL,Brown SH (2006). "Interface terminologies: facilitating direct entry of clinical data into electronic health record systems." J. Am. Med. Inform. Assoc., 13(3): 277-288.
Rui T, Jinshu S, Feng C (2009). Network access control mechanism based on locator/identifier split, IEEE.
Sattarova FY, Kim T (2007). "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security."
Saxena N (2006). Public Key Cryptography Sans Certicates in Ad Hoc Networks, Springer-Verlag New York Inc.
Schridde C, Smith M,Freisleben B (2009). TrueIP: prevention of IP spoofing attacks using identity-based cryptography, ACM.
Shen X, Du Z, Chen R (2009). Research on NTRU Algorithm for Mobile Java Security, IEEE Computer Society.
Sibona C, Brickey J, Walczak S, Parthasarathy M (1899). Patient Perceptions of Electronic Medical Records, IEEE Computer Society.
Smith E, Eloff JHP (1999). "Security in health-care information systems--current trends." Inter. J. Med. Inform., 54(1): 39-54.
Smith GW, Newton RB, McLean VA (2000). A taxonomy of organisational security policies, Citeseer.Smith JP (1995). "Authentication of digital medical images with digital signature technology." Radiology 194(3): 771.
Sriram VSS, Dinesh S, Sahoo G (2010) "Multiplication Based Elliptic Curve Encryption Scheme with Optimized Scalar Multiplication (MECES)." Ratio 104(512): 106.
Staggers N, Thompson CB, Snyder-Halpern R (2001). "History and trends in clinical information systems in the United States." J. Nurs. Scholarsh., 33(1): 75-81.
Stallings W (2010). Cryptography and network security, Prentice Hall.
Stead WW, Hammond WE (1988). "Computer-based medical records: The centerpiece of TMR." M. D. Computing 5(5): 48-62.
Stevens GS, Library Of Congress Washington Dc Congressional Research (2009). Federal Information Security and Data Breach Notification Laws, Library of Congress Washington Dc Congressional Research Service.
Stevens GM, Attorney L (2007). Information Security and Data Breach Notification Safeguards, Library of Congress Washington Dc Congressional Research Service.
Sucurovic S (2007). "Implementing security in a distributed web-based EHCR." Inter. J. Med. Inform., 76(5-6): 491-496.
Suwannalert P, Rattanachitthawat S, Chaiyasut C, Riengrojpitak S (2010). "High levels of 25-hydroxyvitamin D3 [25 (OH) D3] and-tocopherol prevent oxidative stress in rats that consume Thai brown rice." J. Med. Plants Res., 4(2): 120-124.
Takeda H, Matsumura Y, Kuwata S, Nakano H, Shanmai J, Qiyan Z, Yufen C, Kusuoka H, Matsuoka M (2004). "An assessment of PKI and networked electronic patient record system: lessons learned from real patient data exchange at the platform of OCHIS (Osaka Community Healthcare Information System)." Int. J. Med. Inform., 73(3): 311-316.
Tang PC, Ralston M, Arrigotti MF, Qureshi L, Graham J (2007). "Comparison of methodologies for calculating quality measures based on administrative data versus clinical data from an electronic health record system: implications for performance measures." J. Am. Med. Inform. Assoc. 14(1): 10.
Tartary C (2007). "Authentication for Multicast Communication."
Taute B (2009). "DST-funded information security centre of competence."
Teno JM, Sabatino C, Parisier L,Rouse F (1993). "Impact of the Patient Self-Determination Act's Requirement that States Describe Law Concerning Patients' Rights, The." JL Med. Ethics 21: 102.
Thapen N (2006). "The polynomial and linear hierarchies in models where the weak pigeonhole principle fails."
Thomas PN (2009). "Little Brother's Big Book: The Case For A Right of Audit In Private Databases." CommLaw Conspectus, 18: 155-269.
e T, Hildebranda C, Engelbrechta R, Pharowb P, Demskia H, Savastanoc M, Blobelb B, Hovstd A (2006). "BioHealth-Marketing of eID Standards for the eHealth Domain."
Uys L (2009). "Voice over internet protocol (VoIP) as a communications tool in South African business." Afr. J. Bus. Manage., 3(3): 089-094.
, Kuosmanen L, Karkkainen J, Kjervik DK (2009). "Patients' rights to comp lain in Finnish psychiatric care: An overview." Int. J. Law Psychiatry 32(3): 184-188.
Van Bemmel JH, Musen MA (1997). Handbook of medical informatics, Bohn Stafleu Van Loghum.
Van der Haak M, Wolff AC (2003). "Data security and protection in cross-institutional electronic patient records." Inter. J. Med. Inform., 70(2-3): 117-130.
Vincent OR, Folorunso O,Akinde AD (2010). "Improving e-payment security using Elliptic Curve Cryptosystem." Elect. Commerce Res. 10(1): 27-41.
Vogue BIN, Old Y,Deleted E (2010). "Privacy & Data Security Law J. pp.194.
Walia IK (2010). "Infringement of Right to Privacy as a Crime."
Winslade WJ (1982). "Confidentiality of medical records: An overview of concepts and legal policies." J. Legal. Med., 3(4): 497-533.
Zhang R, Liu L (2010). "Security Models and Requirements for Healthcare Application Clouds."
Zimeras S, Diomidous M (2009). "An electronic health record model for the spatial epidemiological analysis of clinical data." Materia Soci Medica, 21(2): 103-9.