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

Hamdan O. Alanazi1,4, Hamid A. Jalab1, Gazi Mahabubul Alam3*, B. B. Zaidan2 and A. A. Zaidan2

1Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia.
2Department of Electrical and Computer Engineering, Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Selangor Darul Ehsan, Malaysia.
3Department of Educational Management, Planning and Policy, Faculty of Education, University of Malaya, 50603 Kuala Lumpur, Malaysia.
4Faculty 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 Iliola, 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 from patients' bedside. In this situation, medical record transmission over an unsecured network poses an unacceptable risk to patient privacy.
from their desks and cumbersome workstations (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 Winslott, 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 (Mcllwraith, 2006; Herb 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; Bouchou and Mostefai, 2009) (Figure 1).
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 website, 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 yen, 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 subsidiarity 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 Legemaatedom 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 Marid (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-100 has 6X smaller key-size than RSA-1024 and can generate a signature 12 times faster than RSA (Balitranas 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 (Siriram 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>
<thead>
<tr>
<th>No</th>
<th>Goal</th>
<th>Drop-back</th>
<th>Year</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Ferreira et al., 2004)</td>
<td>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.</td>
<td>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.</td>
<td>2004</td>
<td>15</td>
</tr>
<tr>
<td>(Brandner et al., 2002)</td>
<td>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.</td>
<td></td>
<td>2002</td>
<td>37</td>
</tr>
<tr>
<td>(Smith, 1995)</td>
<td>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.</td>
<td></td>
<td>1995</td>
<td>16</td>
</tr>
<tr>
<td>(Janbandhu and Siyal, 2001)</td>
<td>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.</td>
<td></td>
<td>2001</td>
<td>33</td>
</tr>
<tr>
<td>(Epstein et al., 1998)</td>
<td>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.</td>
<td></td>
<td>1998</td>
<td>25</td>
</tr>
<tr>
<td>Reference</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Bos et al., 2004)</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Gobi and Vivekanandan, 2009)</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(McGuire and Fisher, 2008)</td>
<td>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 are some points are required further improvements. In additional the technical perspective has not stated. As well, the protection of the electronic patient record has not clearly mentioned.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Anderson, 2000)</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(De Meyer and Lundgren, 1998)</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 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.

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Doctor will treat the patient and the patient will describe his condition</td>
</tr>
<tr>
<td>2</td>
<td>In the medical profession there should be ethics for doctors to follow (there is no punishment for not following).</td>
</tr>
<tr>
<td>3</td>
<td>Doctor knows that no law governing the relationship with the patient and it will be responsible when abused his powers to act in.</td>
</tr>
<tr>
<td>4</td>
<td>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</td>
</tr>
<tr>
<td>5</td>
<td>The patient has powers of access to his medical records.</td>
</tr>
<tr>
<td>6</td>
<td>The law can protect the rights of the patient.</td>
</tr>
<tr>
<td>7</td>
<td>The law regulates the protection of the patient and the powers of access to medical records relating to the accounting and responsible for misuse.</td>
</tr>
<tr>
<td>8</td>
<td>Will analyze and prepare the law to be applied.</td>
</tr>
<tr>
<td>9</td>
<td>To access the security requirements must be analyzed Law.</td>
</tr>
<tr>
<td>10</td>
<td>To implement the security requirements on the medical records of patients must be used in computer science.</td>
</tr>
<tr>
<td>11</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 3. Critical review.

<table>
<thead>
<tr>
<th>Paper</th>
<th>Security Objectives</th>
<th>Algorithms</th>
<th>Protection of patient’s privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Blobel 2000)</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Gritzalis 2007)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Espinosa 1998)</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>(Bos 1996)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Blobel and Roger-France 2001)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Pharow and Blobel 2005)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Kluge 2007)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>(Ahmad 2009)</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
</tr>
</tbody>
</table>

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.

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

Figure 2. The life cycle of EMR.
security 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; Asymmm, 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


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


Social Science & Medicine.


Bonet ML, Pitatsi T, "No Feasible Interpolation for TC." Cryptogr., 229.


Hodge MH (1987). History of the TDS medical information system, ACM.


Izet Masic HP (2007). Requirements for Security and Privacy, Pro...
Perrig A (2001). The BiBa one-time signature and broadcast authentication protocol, ACM.