CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter examined previous studies related to security and privacy of using Electronic Health Records (EHRs) or also known as Electronic Medical Records (EMRs). EMRs is defined as the Electronic Medical Records system that collect, store and display patient information. They are means to create legible and organized recordings and to access clinical information about individual patients. Furthermore, researcher also demonstrated some of the models currently in use by medical organizations as well as other means that were highlighted in earlier studies.

2.2 APPLICATION OF PRIVACY, SECURITY AND ETHICS IN ISLAM CONCERNING ICT

In accordance with the provisions of Islamic Shari researcher, part of research explained about security issues and privacy of legitimate perspective, and the perspective available so that they can describe these things. From the Islamic perspective, guiding principles in ICT must be based on Islamic Philosophy which is from al-Qur'an and as-Sunnah. There are three divisions derived from the ICT guiding principles ethics security and privacy as shown in Figure 2.1 (Mohd Fauzan, 2013).

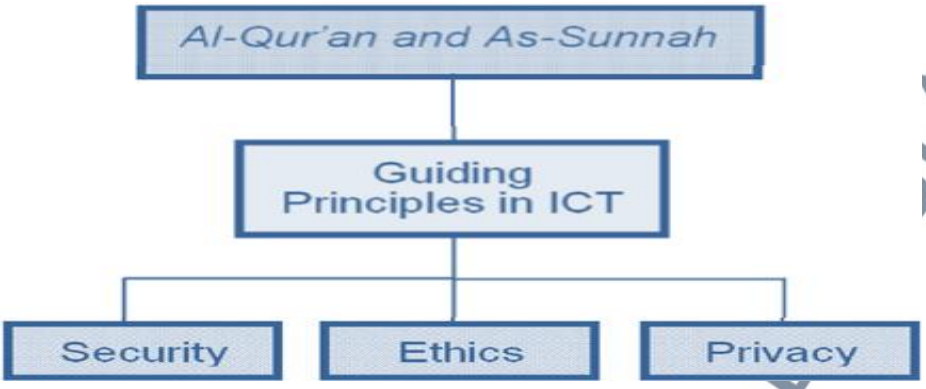

Figure 2.1: Model for Ethics, Security and Privacy from Islamic Perspective (Source: Mohd Fauzan, 2013)

Privacy from Islamic view respects the privacy of each Muslim including child. Allah S.W.T says in Surah An-Nur verse 27: "O ye who believe! Enter not houses other than your own, until you have asked permission and saluted those in them" And in Surah Al-Hujurat verse 12:"O ye who believe! Avoid suspicion as much (as possible): for suspicion in some cases is a sin: And spy not on each other behind their backs. Would any of you like to eat the flesh of his dead brother? Nay, ye would abhor it...But fear Allah. For Allah is Oft-Returning, Most Merciful. " From these two verses in the Qur'an, it can be concluded that Islam emphasizes the importance of privacy. Islam teaches us to respect the rights of others. Invasion of privacy gives a major impact on the society.

2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPPA)

The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishes, for the first time, a set of national standards for the protection of certain health information. The United States Department of Health and Human

Services (HHS) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Privacy Rule standards address the use and disclosure of individuals' health information — called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used (Murphy, 2008).

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

2.4 EVALUATION ON EHR AND HIE ADOPTION STATUS AND POLICY IMPLEMENTATION

In the 2000's the World Health Organization declared the French healthcare system was the "the best health system in the world". However, in terms of EHR use, it does not have the highest use rates. In fact, EHR is used by about 60% of all general practitioners, but HIE is rare in France (Artmann et al., 2010).

In Spain, many general practitioners have a single computer in their practice, shared by several physicians. HIE is not commonly used for medical information or for administrative data (Corbellini et al., 2010).

In Denmark, a virtual private network (VPN) has been established for the healthcare sector. Most general practitioners and pharmacies use EHR, in addition, many of the specialists in the country use the EHR as well (Kushniruk et al., 2010).

Implementation of EHR has not included all of England, many stakeholders have not yet adopted the system which makes the HIE function difficult to achieve in England (Sheikh et al., 2011).

In 2009, China launched an EHR architecture within the Chinese healthcare system. Currently, the Chinese standards for security and privacy are relatively low (Xu et al., 2011).

In 2012, Austria launched a personally controlled EHR designed to allow more active participation on the part of patients and thus increase rates of implementation. Most general practitioners use this system, but patients are free to choose to use it or not (Pearce and Bainbridge, 2014).

A comparative study of primary care physicians in the Netherlands and Germany showed that EHRs exist but are not yet interoperable, implementation was overseen by health insurance funds in each state. Only half of the physicians who have an EHR have an internet connection to their EHR to potentially exchange information via HIE. However, in fact, only 4% from them share medical information (Schacht, 2014).

Experiences from Denmark, Finland and Canada in moving towards regional and national evaluations of health information system usability where many versions of EHR are from the U.S. Canada has some privacy and safety issues with the EHR systems. It is important to design an EHR system and HIE network that are compatible

with the healthcare system in Canada (and will handle all of the privacy issues) (Kushniruk et al., 2014).

A research on the use and characteristics of electronic health record systems among office-based physician practices in United States from 2001–2013 in the US showed that the implementation rates of an EHR system among general practitioners is about 78% whereas 69% of all physicians are associated with Medicaid or Medicare EHR incentive programs (Hsiao et al., 2014).

Researcher research focused on the importance of using electronic medical records while maintaining security and privacy using a risk analysis framework in addition to encryption technologies.

2.5 EXISTING ONLINE HEALTH MANAGEMENT SYSTEMS

This literature review is based on the examination of some related systems that are actually exist online that provide health management services. Researcher investigation was related to features that need to be provided by a health management system, such as attractive design, pages access speed and features accessibility. This review was done for the following systems.

2.5.1 iCure

Icure is a health management website in Netherlands, it contains a registration form, normal pages access speed and all the features are accessible from the main page as shown in Figure 2.2. There is no staff list which is a lack for a health management web site. The design is not attractive and there is also no treatments list and no patient's file.

Figure 2.2: Model for iCure (Source: Taktik, 2011)

2.5.2 Osoft Health Management

Osoft is a health management website for a hospital located in Paris in France. This site contains appointment form with attractive design and good pages access speed, all features are accessible as shown in Figure 2.3. Osoft lacks on staff list implementation, registration form, treatments list and patient's file.

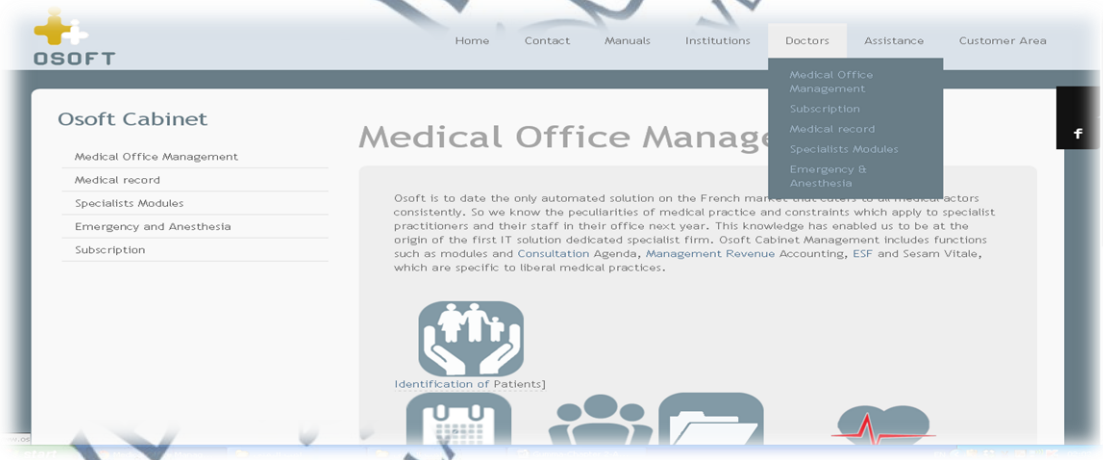

Figure 2.3: Model for Osoft (Source: OSOFT, 2016)

2.5.3 Canadian Medical Association (CMA)

Canadian Medical Association (CMA) is a Canadian health management web site. This site contains appointment form, it is well designed and the speed to access pages is acceptable, all features are accessible and maintains a staff list as shown in Figure 2.4. This site lacks on providing registration form and it does not maintain a patient's file.

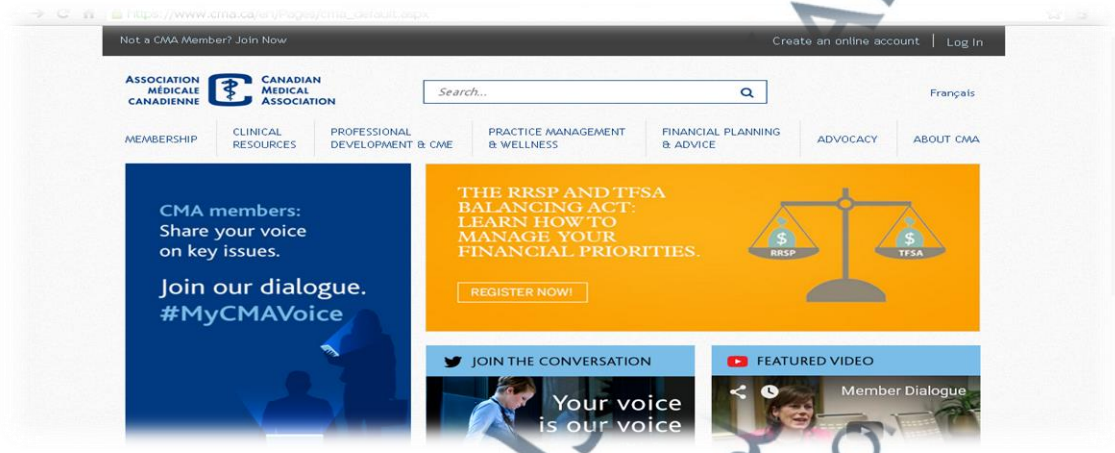

Figure 2.4: Model for Canadian Medical Association (Source: Canadian Medical Association, 2016)

2.5.4 Electronic Health Solutions (EHS)

Electronic Health Solutions (EHS) as shown in Figure 2.5 was developed to facilitate efficient and high quality health care in Jordan through nationwide implementation of an electronic health record solution. Security features in EHS includes a Personal smartcard coupled and Personal identification number. As for the disadvantage is that it requires a long time to verify the e-holder whom contacted server outside the hospital.

Figure 2.5: Model for Electronic Health Solutions (Source: Electronic Health Solutions, 2014)

2.5.5 Chan Soon-Shiong Medical Center at Winber (CSMCW)

Chan Soon-Shiong Medical Center at Winber (CSMCW) is a website that patient can securely view their health information online from the hospital system. Security features in the CSMCW includes Password policy. However, if Universal Password or Advanced Password Rules are not enabled, password policies are not enforced, and passwords on connected systems cannot be reset. Figure 2.6 shows the interface of the system.

Figure 2.6: Model for Chan Soon-Shiong Medical Center at Winber (CSMCW) (Source: Windber Hospital Inc., 2016)

2.5.6 St. Mary's Health Care System

St Mary's is an Internet application that provides a patient with secure web based access to their electronic medical record at Trinity Health and its subdivisions as shown in Figure 2.7. Security in this system uses encryption technology designed to help ensure the integrity and privacy of the information. As an added security precaution, all data is kept on servers with firewalls that meet or exceed industry standards to prevent intruders from gaining access to the system. As for the disadvantage in this system is that SSL encrypt the information that a patient send through the server and it takes more server space than if the information weren't encrypted.

Figure 2.7: Model for St. Mary's Health Care System (Source: St Mary's, 2016)

2.5.7 Carolinas HealthCare System

Carolinas HealthCare System uses industry accepted security practices so that the system is protected and information remains secure. Among security measures implemented in the system is using encryption technology such as Secure Socket Layer (SSL). Figure 2.8 shows the interface of the system.

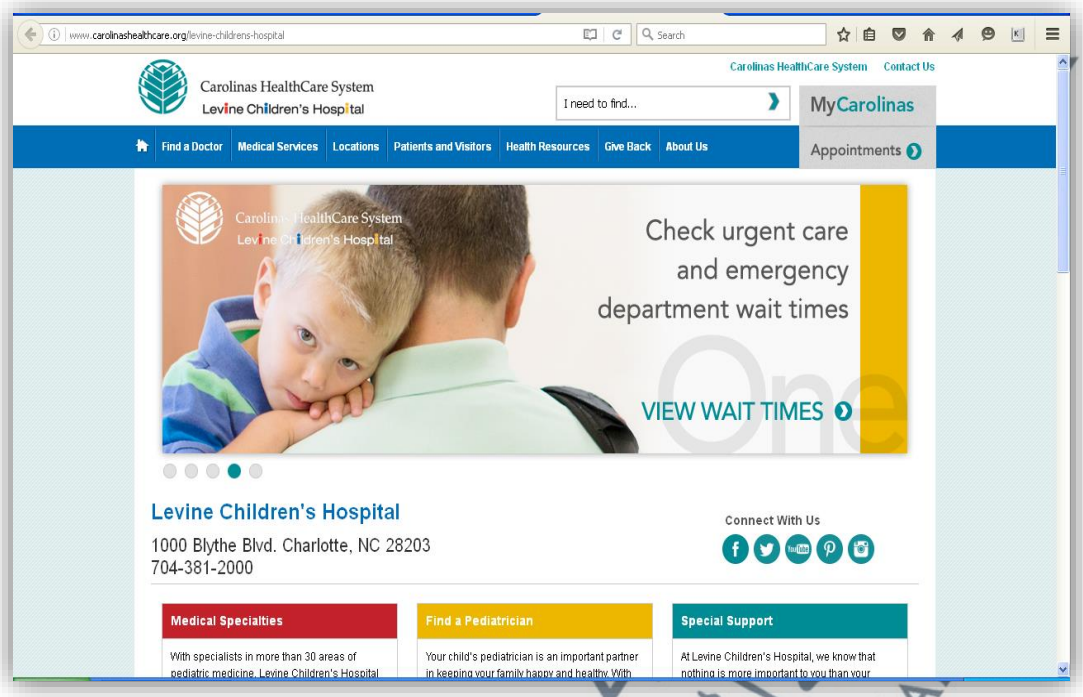

Figure 2.8: Model for Carolinas HealthCare System (Source: Carolinas HealthCare System, 2016)

2.5.8 VorroHealth

VorroHealth was developed to facilitate efficient and high quality health care in Jordan through nationwide implementation of an electronic health record solution as shown in Figure 2.9. Security features in the VorroHealth includes cookies to log IP addresses and browser information for the purposes of system administration and user functionality. This system has a tracking feature to log user activity.

Figure 2.9: Model for VorroHealth (Source: Vorro Inc., 2016)

2.5.9 Health Management System (HMS)

Researcher have developed the system to maintain medical records about all patients and provide services such as use medical record to follow-up of each patient by the doctors and allow the patient to make appointment as shown in Figure 2.10. The administrator can create new staff and edit the staff list, allow the doctor to prescribe medicines, show the medical acts of the patient through the medical report, as well as security and privacy, which was added to the system. Researcher also added some features that were missing in the existing systems and implement services needed by a health management system. Table 2.1 shows a simple comparison between researchers' system and other aforementioned systems.

Figure 2.10: Model for HMS

Table 2.1 Features Comparison Between Existing Systems and HMS

Features	iCure	Osoft	CMA	EHS	CSMCW	St. Mary	Carolinas	Vorro Health	HMS
Registration form	*	√	*	*	√	√	√	*	√
Appointment form	√	*	√	√	*	√	*	*	√
Attractive design	√	*	√	√	√	√	√	√	√
Pages access speed	√	√	√	√	√		√	√	√
Features accessibility	√	√	√	√	√	*	√	√	√
Staff list	*	*	√	√	√	*	√	√	√
Treatment list	*	*	√	*	√	*	√	√	√
Patient's file	*	*	*	*	√	√	√	*	√
File encryption for patient	*	*	*	*	√	√	√	*	√
Database encryption	*	*	*	*	*	√	*	*	√
Login audit	*	*	*	*	*	*	*	*	√
Access control	*	*	*	*	*	*	*	*	√
Password attempts limitation	*	*	*	*	√	*	*	*	√

Based on Table 2.1, it can be concluded that most of the system lack security element in their system such as file encryption for patient, database encryption, login audit, access control and password attempts limitation. These are security practices to eliminate the abuse of these systems by hackers, as well as to protect data privacy of the users, either doctors or nurses or patients. Therefore, HMS was created to overcome the gap of these security elements in the hospital management system.

2.6 TRIPLE DES IMPLEMENTATION IN A SYSTEM

Triple DES or 3DES or TDES have been widely implemented and tested in various systems. Researcher's system also implemented Triple DES as security measures. Below are some research regarding 3DES.

Jenkins et al. (1977) presented instruction set architecture extensions and hardware designs for TDES implemented on a multi-threaded SDR (Software-Defined Radio) platform, and investigated their impacts on area, performance, and power. The results indicated that the proposed extensions improved the performance of TDES by a factor of 39 and reduce energy by 97%, while increasing average power by only 34%. They proposed an ATM (Automatic Teller Machine) PIN (personal identification number) Pad system that was designed based on 3DES encryption algorithm, and the exception handling is added in the PIN Pad (such as: jitter, command coverage, the wrong password more than three times). The experimental results demonstrate feasibility of designed system to ensure that the PIN will not be leaked and protect user information effectively. 9-pin serial port is used in interface of the circuit. User can upgrade via USB interface. Software includes abnormal processing. User can be reminded when the abnormal problem appears in the system. And the software can be updated online. The

PIN Pad is still used in replacement of the hardware and software. There are some detecting programs in the software, which help the PIN Pad software upgrade to make the keyboard more secure. In this design, password peep.

Liu and Yang (2010) conducted a research on the implementation of 3DES based on Web Services Security Model. It uses 3DES algorithm to encrypt the SOAP message to prevent the leakage of the sensitive data in order to ensure its confidentiality. In the algorithm selection: 3DES key length from the DES, 56bit into a 112bit, even 128bit, and DES operations was carry out thrice. It has greatly improved the data security to deal with a strong attack and it is relatively safe. However, due to the use of the transposition, replacement, and XOR encryption method, its encryption speed is relatively slow. In the computing speed it's about 3 times slower than the DES algorithm and this affects the quality of service (QoS). Therefore, MD5 is implemented in the system. MD5 Algorithm stands for the Message Digest algorithm5 that is equal to Hash Function for the purpose of Integrity. It is designed to be quite fast on 32-bit machines. In addition, the MD5 algorithm does not require any large substitution tables and the algorithm can be coded quite compactly. As it can be seen from the experimental platform, this paper embed the MD5 algorithm digital signature. It ensures that the message during transmission will not be tampered in order to achieve data integrity for sensitive data. MD5 Algorithm is used to sign the IP address and request message. Then it sends the results of safe handling to the server (Service Provider). When the server (Service Provider) receipts of the message, it will decrypt the IP Address using its Private and calculates its hash to identity authentication of the request message. If the verification is successful, it will uses the key to decrypt the request message. Then, it will verify the validity of the signature. If the signature are valid, it will complete their

permission authenticate in the security domain. If all that above are right, it will establish a session and contact the Web services. It will encrypt and sign the response message. Then add to the time stamp, IP address and session ID and send them to the client.

Navneet and Vijay (2012) explained how the data transactions can make more secure with different security techniques used in ATM transactions. Various security levels of data and encryption standard used in banking data transaction security. Encryption methods are built into the communication network to prevent unauthorized transactions that could protect the data from unauthorized access. This paper focused on Data Encryption Standard and Advanced Encryption Standard, these are the encryption standards used by the banks to protect the data and for secure data transmission. The results shown that AES able to process six times faster compared with the triple DES for the same processing capacity. In addition, when compared with AES, triple DES implementation is more suitable for application on the device hardware, such as network system communications, VPN network devices or at an ATM.

Tsague et al. (2012) proposed an Advanced Mutual-Authentication Algorithm using 3DES for Smart Card Systems. This paper proposes an advanced mutual-authentication protocol for security and privacy protection with smart card systems using a 3DES algorithm as a cryptographic primitive. This protocol protects high-valued goods against attackers with mutual authentication. Authentication scheme involves three entities (the user's smart card, the smart card reader and the backend server) and consists of three phases: the registration phase, the login and authentication phase, and the password update phase. To access the provided services, the user has to first register with the backend server. During this phase, the user is issued with a personalized smart

card with a default password. The login phase is executed at the smart card reader and the authentication verifies the authenticity of the backend server, the smart card reader and the user's smart card. As for the password update phase, it is completed only at the user's terminal.

Seok and Sang (2013) conducted a research on Optical implementation of Triple DES Algorithm Based on Dual XOR Logic Operation. In the schematic architecture, the optical 3DES system consists of dual XOR logic operations, where XOR logic operation is implemented by using a free-space interconnected optical logic gate method. The main point in the proposed 3DES method is to make a higher secure cryptosystem, which is acquired by encrypting an individual private key separately, and this encrypted private key is used to decrypt the plain text from the cipher text. Schematically, the proposed optical configuration of this cryptosystem can be used for the decryption process as well. The major advantage of this optical method is that vast 2-D data can be processed in parallel very quickly regardless of data size. Of course, the proposed dual XOR optical encryption method provides higher security strength to use double key encryption, and has an advantage of simple optical setup configuration. The proposed method seems to perform 2,048 DES blocks or 1,024 3DES blocks cipher. Besides, because the key length is equal to 512×256 bits, $2\ 512 \times 256$ attempts are required to find the correct key. Computer experiments verified that the proposed method is perfect and suitable for cryptographic applications and secure communication system.

Karthik and Muruganandam (2014) provided a performance comparison between the most common encryption algorithms: DES, 3DES, AES and Blowfish. Their presented simulation results showed that 3DES has a better performance result with ECB and CBC (Chain Block Chaining) than other common encryption algorithms used. In their

paper, they presented a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, Blowfish, RC2, and RC4. In case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption.

Saranya and Shankar (2014) studied an enhanced attribute based encryption with multi-parties access in cloud area. This paper has secured information sharing, Attribute Based Encryption (ABE) and Triple Data Encryption Standard (Triple DES) as basis of the solution to use PHR files to support strategic objectives. Examples was not discussed in this paper but included Predicate Encryption where the attributes are encrypted and Functional Encryption allowing greater generality in attributes/policies. In the longer term Functional Encryption could lead to the prospect of cryptographically controlled reduction. This paper has outlined how ABE may be used by secure information sharing with both ABE adopters and legacy. The benefits of this approach are improved security within domains, mainly by reducing the attack surface for insiders and malware, and also by minimizing dependency upon critical cryptographic servers. Triple DES reduces the impact of risks associated with errors and compromise of egress data guards, and scenarios have been identified these benefits could lead to improved security.

Jagyasi and Pimple (2014) proposed Security Enhancement in Cloud Computing Using Triple DES Encryption Algorithm. The 3DES algorithm uses eight bytes per block. So the user will enter the different 24 bytes key to be used in the algorithm. The confidential 3DES key combined between the corresponding parties is appropriately 168-bits lengthy. This key comprises of 3 self-sufficient 56-bit numbers utilized by the DES algorithm. All of the 3 56- bit sub keys is placed as a 64-bit (8 octet) quantity, with the lowest possible significant bit of every octet used as a parity bit. The 3DES encryption algorithm requires 3, 8 byte keys for encryption

and decryption process. The user enters the key while registration for the cloud access i.e. when the user makes registration to access the cloud, the user has to choose the key which will be used as the key encryption and decryption of the user data. This will make the user to remember the key easily.

Nisha and Neetu (2015) proposed "Suspicious Email Detection System" to provide a way to identify the criminal activities. The proposed method used cryptography algorithm triple DES (3 Data Encryption standard) it is very fast algorithm for encrypt or decrypt the information (email message) in a successful rate. Triple DES Algorithm used by admin to encrypt the messages sent to the users or sent some warnings about the other user's suspicious activity. Suspicious words dictionary is used to detect the suspicious words which are not actually used in the normal messaging or communication.

Table 2.2: 3DES Literature Comparison

Article/s	Objective	Methodology	Results
Jenkins et al. (1977)	Set architecture extensions and hardware designs for TDES implemented on a multi-threaded SDR platform, and investigates their impacts on area, performance, and power.	Novel instruction set extensions and hardware designs for TDES that provide significant performance and energy benefits while maintaining flexibility in key processing	Improve the performance of TDES by a factor of 39 and reduce energy by 97%, while increasing average power by only 34%.
Liu and Yang (2010)	The implementation of 3DES based on Web Services Security Model. It uses 3DES algorithm to encrypt the SOAP message to prevent the leakage of the sensitive data in order to ensure its confidentiality.	In the algorithm selection: 3DES key length from the DES, 56bit into a 112bit, even 128bit, and DES operations was carry out thrice. It has greatly improved the data security to deal with a strong attack and it is relatively safe.	However, due to the use of the transposition, replacement, and XOR encryption method, its encryption speed is relatively slow. In the computing speed it's about 3 times slower than the DES algorithm and this affects the quality of service (QoS). Therefore, MD5 is implemented in the system. MD5

Article/s	Objective	Methodology	Results
			Algorithm stands for the Message Digest algorithm5 that is equal to Hash Function for the purpose of Integrity.
Navneet and Vijay (2012)	In order to make communication security from ATM to Bank and from Bank to ATM a new level of security emerge.	Data Encryption Standard and Advanced Encryption Standard, these are the encryption standards used by the banks to protect the data and for secure data transmission.	Triple DES implementation is more suitable for application on the device hardware, such as network system communications, VPN network devices or at an ATM.
Tsague et al.(2012)	An advanced mutual-authentication protocol for security and privacy protection with smart card systems using a 3DES algorithm as a cryptographic primitive.	This protocol protects high-valued goods against attackers with mutual authentication. Authentication scheme involves three entities (the user's smart card, the smart card reader and the backend server) and consists of three phases: the registration phase, the login and authentication phase, and the password update phase. To access the provided services, the user has to first register with the backend server.	This protocol protects high-valued goods against attackers with mutual authentication.
Seok and Sang (2013)	Optical implementation of a 3DES algorithm based on dual XOR logic operations for a cryptographic system.	3DES method is to make a higher secure cryptosystem, which is acquired by encrypting an individual private key separately, and this encrypted private key is used to decrypt the plain text from the cipher text. Schematically, the proposed optical configuration of this cryptosystem can be used for the decryption process as well. The major advantage of this optical method is that vast 2-D data can be processed in parallel very quickly regardless of data size.	Attempts are required to find the correct key. Computer experiments verified that the proposed method is perfect and suitable for cryptographic applications and secure communication system.
Karthik and Muruganandam (2014)	Provide a performance comparison between the most common encryption algorithms: DES, 3DES, AES and Blowfish.	They presented a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, Blowfish, RC2, and RC4. In case of changing key	Showed that 3DES has a better performance result with ECB and CBC (Chain Block Chaining) than other common encryption algorithms used.

Article/s	Objective	Methodology	Results
		size, it can be seen that higher key size leads to clear change in the battery and time consumption.	
Saranya and Shankar (2014)	Triple DES reduces the impact of risks associated with errors and compromise of egress data guards, and scenarios have been identified these benefits could lead to improved security.	Include Predicate Encryption where the attributes are encrypted and Functional Encryption allowing greater generality in attributes/policies .In the longer term Functional Encryption could lead to the prospect of cryptographically controlled reduction. Has outlined how ABE may be used by secure information sharing with both ABE adopters and legacy.	Triple DES reduces the impact of risks associated with errors and compromise of egress data guards, and scenarios have been identified these benefits could lead to improved security.
Jagyasi and Pimple (2014)	Security Enhancement in Cloud Computing Using Triple DES Encryption Algorithm.	The 3DES encryption algorithm requires 3, 8 byte keys for encryption and decryption process. The user enters the key while registration for the cloud access i.e. when the user makes registration to access the cloud, the user has to choose the key which will be used as the key encryption and decryption of the user data. This will make the user to remember the key easily.	The user will register and will get the cloud space. While registering the user has given the key which will be used as encrypted and decrypted purpose. As the user will register its space will be created and after validating the account the user can store the files and documents in the encrypted form. The user is able to upload all the files and can maintain the security of the data. The user will also be able to upload images and videos in its space. This will also be encrypted using the encryption algorithm so that the authentication of the cloud user will be maintained and security of the files and images will be done.
Nisha and Neetu (2015)	Detect the suspicious mails sent from the users who are already registered on Suspicious Email Detection System via Triple DES Algorithm.	Suspicious words dictionary is used to detect the suspicious words which are not actually used in the normal messaging or communication.	Triple DES Algorithm used by admin to encrypt the messages sent to the users or sent some warnings about the other user's suspicious activity. Admin created the data dictionary of suspicious words to help detect the suspicious activity of the users.

2.7 HOSPITAL MANAGEMENT SYSTEM SECURITY FRAMEWORK

The framework shown in Figure 2.11 is composed of several activities and industry best practices that provide a mechanism for the HMS to:

1- Describe current security posture;

2- Describe the target state for cybersecurity;

3- Identify and prioritize opportunities for improvements;

4- Assess progress toward the target state;

5- Communicate among internal and external stakeholders about cybersecurity risk.

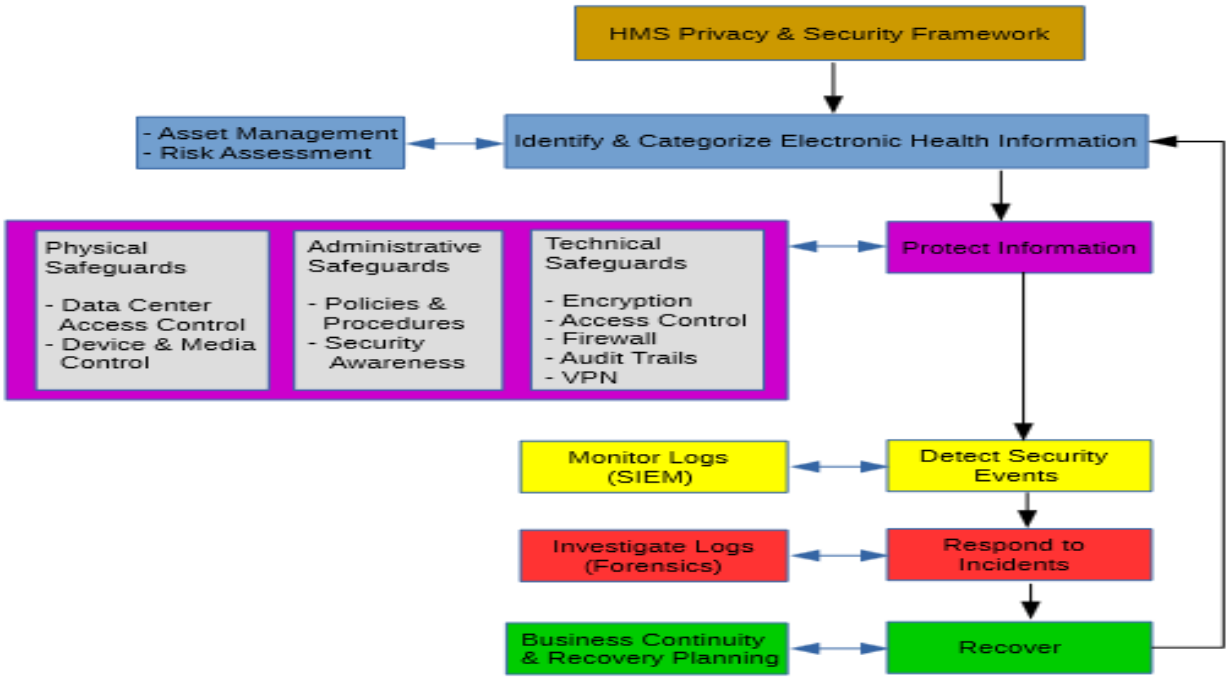

Figure 2.11: Hospital Management System Security Framework (Source: NIST, 2014)

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy,

business, and technological approaches to managing that risk. It can manage cybersecurity risk across the entire HMS organization.

2.7.1 Technical Safeguards

Major security elements that should be addressed include prevention of unauthorized access to patient's medical records (confidentiality) prevention of unauthorized alterations or loss to data (integrity) and prevention of compromises to availability of data to authorized individuals. Hence incomplete or unavailable data is not considered secure. In order to develop an effective security program, security measures must be designed to allow authorized end-users access to information in a timely manner (Golightly & Tuthill, 2012). Some of technical safeguards for Hospital Management System are as explained below.

2.7.1.1 Encryption

A proper encryption scheme must be introduced in order to achieve confidentiality in an EHR system. If the server itself holds the private key, then key symmetric schemes are also vulnerable, as the key might be stolen along with the encrypted data. Encryption key should be hosted on a separate physical server to prevent decryption of patient data if the data storage machine is ever compromised. When accessing EHR data over the Internet then a secure connection such as SSL/TLS should be used to guarantee the transmitted data is encrypted.

2.7.1.2 Access Control

User authentication can be defined as the way in which users prove their authenticity to the EHR. Username or identity (ID) with an associated password have been the most common user authentication mechanisms in EHRs (Fernandez-Aleman et al., 2013).

It is advisable to use a central authentication server (such as Microsoft LDAP), so all users' access should be controlled within a group policy, where a person can apply password , login rules and policies through the centralized authentication server.

2.7.1.3 Audit Trails

Audit trails are an important tool for data security in EHR systems. However, audit trails are only a palliative measure, since the confidentiality or integrity of the information can be violated before countermeasures have been taken. Review shows that many systems rely on the auditing of log data as a security mechanism. Audit trails can serve as proofs when disputes arise regarding serious issues such as abuse of permissions, illegal access attempts, and the improper disclosure of patients' health data.

Audit trails can become a fundamental data security tool, as some security breaches have resulted from the misuse of access privileges by authorized persons. Examining access logs is often an overwhelming task. Audit trails may not be practical, since they can exceed the size of the original file by orders of magnitude. Hash chains are currently the most promising approach for storing authentic log files with a reasonably small overhead (Fernandez-Aleman et al., 2013).

2.7.1.4 VPN

Healthcare industries are interested in Virtual Private Network (VPN) technology because it promises low-cost, secure data transmission via the Internet and can be used to replace long- distance telephone charges and dedicated lines. VPN supports secure solution for mobile users. VPN is based on Internet Protocol Security (IP Sec) which provides added security features. IP Sec includes such security measures as authentication, encryption and key management. VPN setup needs two configuration files. The first one is the security – level definition and the second one is secure network map files. The security level definition contains parameters like the types of authentication, encryption scheme and so on. The secure network map file specifies which gateway is responsible for which remote VPN node. VPN offers a number of authentication schemes such as Handshake Message Authentication code, RSA Data Security public-Key cryptosystem, Message Digest 5, Secure Hash Algorithm and shared secret. Encryption technologies supports Blowfish algorithm, Data Encryption Standard (DES), Triple DES, International Data Encryption Algorithm, RSA, and RC5. VPN security related to Electronic Healthcare Monitoring System (EHMS) includes healthcare records like EHR, EMR, PHR sharing and integration in healthcare clouds and analyzing the arising security and privacy issues in access and management of healthcare data. VPN Security encompasses the collective measures that ensure healthcare data and transmission security within a VPN connection over a public network. It includes security methodologies and tools that ensure communication confidentiality, user authentication and message integrity in a VPN (Parameswari and Prabakaran, 2015).

2.7.1.5 System Backups

Hardware or software failures, including "denial-of-service" attacks, can cause downtime or loss of vital health care data for EMR users. The reliability of EMR systems and data should be considered a security concern and should be covered in security policy and system management activities, usually through mechanisms that support data redundancy and system backups (Gumma and Fauziah, 2014).

2.7.2 Administrative Safeguards

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information. (Federal Register, 2013).

2.7.3 Physical Safeguards

Physical safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

2.8 CONCLUSION

In this chapter researcher have reviewed previous studies related to the use of electronic medical records from 2010-2015 and their results. Some of the health portals on the Internet were also discussed as well as presenting a security framework to increase the security and privacy of the EMR.