Levels of Protection in using Cloud Computing in Health Sector under Islamic and Saudi Laws

Emna Chikhaoui
Prince Sultan University, College of Law, Prince Nasser Bin Farhan Street, Riyadh, Saudi Arabia

Keywords: Cloud Computing, e-Health, Protection, Privacy, Security, Legislation.

Abstract: The implementation of cloud computing in the context of health information provides a hardware independent manner of accessing, sharing data, streamlining costs and optimizing efficiency. Despite the benefits provided by cloud computing, the process of migrating from a health care IT system remains slow and subject to privacy and security challenges. In this paper we explore the levels of protection in using the clod in health sector under Islamic law and Saudi legislation.

1 OBJECTIVES OF RESEARCH

To present the opportunities and challenges of cloud computing in health organizations.

To discuss privacy under Islamic law which may hinder the adoption of health care cloud computing.

To analyse current privacy and data protection laws in Islamic and Saudi legislation.

To suggest measures that may enhance the viability of cloud computing.

2 METHODOLOGY

The purpose of this research paper is to analyze the viability of health care cloud computing in the context of Saudi and Islamic privacy legislation. To achieve this objective, we use the following methodology:

Content analysis where literature and laws; including Islamic law and Saudi legislation regarding privacy and security concerns were analyzed.

3 FINDINGS

Cloud computing represents a paradigm shift in healthcare IT. However current data center IT is resistant to change as a consequence of privacy, data protection and data reliability concerns, as well as Saudi Arabia's complex jurisdiction. Thus in addition to raising consumer awareness on cloud computing, the legislation of privacy, confidentiality and security remain obstacles to be overcome.

4 INTRODUCTION

Cloud computing is an emerging technology with the potential to revolutionize health care services, however one must observe a series of principles before moving safely to the cloud.

The public should be aware of health information privacy, confidentiality and security of health data. Legislators continue to regulate the ever changing field of health informatics.

The Health Insurance Portability and Accountability Act of 1996 (HIPPA) mandates the development of a national privacy law, security standards and electronic transactions standards and provides penalties for standards violations and wrongful disclosures of health information (Chandra and Adesh, 2013).

Other contributions to public awareness of privacy and data security rights include the 1995 European Union's Enactment of the Data Privacy Directive, officially Directive 95/46/ EC on the protection of individuals with regard to the processing of personal data within the European Union and the free movement of such data. The General Data Protection Regulation adopted in April 2016 has superseded the Data Protection Directive and became enforceable on 25 May 2018. However,

Chikhaoui, E.
Levels of Protection in using Cloud Computing in Health Sector under Islamic and Saudi Laws.
DOI: 10.5220/0007232704310437
In *Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2018) - Volume 1: KDIR*, pages 431-437
ISBN: 978-989-758-330-8

in Saudi Arabia privacy law in the context of information security and consumer data protection is yet to be legislated and implemented. This paper addresses the issues of privacy, confidentiality and security of health care cloud computing through the perspective of Islamic and Saudi Law.

5 SOURCES AND GENERAL PRINCIPLES OF PRIVACY UNDER ISLAMIC LAW

One should note that all religious texts from the Quran or the Sunnah lie at the highest level of authoritativeness as sources of law in Islam. This makes the implications of their language a ready material for legal principles to be derived from. Whilst the term “privacy” is not explicitly referred to in the Quran, it contains verses emphasizing the importance of the individual right to privacy.

Several Quranic verses emphasize individual's right to privacy. The most prominent of these are two verses referring to the privacy of the home: “O you who have attained to faith! Do not enter houses other than your own unless you have obtained permission “hatta tasta’nisu" and greeted their inmates” (Asad, 2008). These excerpts evidence the textual basis for privacy protection as applied to privacy in the household. Additionally, the Quran establishes a right to privacy for people vis-à-vis their family members, that is, within their own home. The Quran (24: 58) specifies three times at least when explicit permission has to be taken before people could enter into the private domain (room, etc) of their parents: before the dawn prayer, during the afternoon (possible time for napping), and after the night prayer.

This Quranic principle applies to all Muslims, but young adults who have recently reached the age of puberty are simply encouraged in this verse to get accustomed to the habit of seeking permission when they want to enter rooms other than theirs, so that such becomes second nature to all members of the family. The Prophet of Islam has emphasized the duty of protecting the privacy of people’s correspondence and communication whether or not they take place in a private place. The Prophet is reported to have said “He, who looks into a letter belonging to his brother, looks into the hellfire.” (Bin Asha’th, 2008).

This establishes that, even if a private communication is conveyed outside of a private environment, the nature of the correspondence creates a right to privacy that must be applied to the correspondence. The forgoing Quranic verses and Sunnah of the Prophet establishes the very basis of right to privacy and its utmost importance. Moreover, if a Muslim has committed a crime and the investigation could potentially breach his privacy, the Prophet very clearly advises not to proceed with the investigation. Thus, the texts from Quran and Sunnah of the Prophet suggest that the practice of deploying modern technologies by the present governments in breach of privacy is to be considered as un-Islamic.

The Islamic principles on privacy can be summarized as follows: (Muhammad, 2011). Every man and woman has certain information for which they have the right and obligation to keep secret. The extent of secrecy changes according to the nature of the observer, the time of observation, and the amount of information observed. Some of the secrets can be joint secrets and all the parties have the obligation to keep it secret. Some of the secrets can be shared (disclosed to someone else) but the nature of the observer is conditional (who the someone could be?) and then the one who receives it has the obligation to keep it secret. It is undesirable to investigate the secrets of someone else and intrusion into the privacy of someone else is punishable by law.

5.1 Privacy: A Sharia Law Perspective

As per the earlier discussion on the concept of privacy in Islam, one can figure out that right to privacy has not been introduced as a distinctive, well-defined legal term in Islamic legal manuals. Islamic juristic language indicates that the privacy of the individual constituted one of Muslim jurists’ concerns. In Islamic legal literature one may find references to Quranic Ayats and Hadiths of the Prophet establishing privacy aspects of what is considered in contemporary legal terms as the right to privacy.

Protection for the individual privacy has not been totally neglected in Islam as evidenced in the Quran and Sunnah of the Prophet (sources of Islamic Law) establishing the right to privacy. In fact, scholars of Islamic law have paid considerable attention to the topics related to the different aspects of privacy. The sanctity of one's body privacy is recognized in Islamic law and the Quran (24-58) demarcates certain periods in a day which are times of privacy for an individual and indicates the need for prior permission before entering the private premises of another. These periods are before the prayer at

dawn, during the afternoon where one needs to rest and also after the night prayer.

In addition, domestic privacy is also considered an important facet of Islamic life and this idea permeates different aspects of Sharia. Moreover, privacy as to proprietary interests was the first legal aspect of privacy recognized by the Muslim jurists. In fact, the Quran (24:27-8) forbids entering another's house without prior permission. It is understood that recognizing privacy in the domestic domain is not just illegal, but it may be also considered as an intrusion into matters of sensitivity which may enlarge the scope of privacy in Islamic law.

Islamic Law offers protection for privacy as shown in Quran and Sunnah, however, attempts should be made at articulating the general principles of classical Islamic Law and addressing the emerging challenges of technological evolution. (Rehman, 2017). Moreover, the studies reveal that in classical Islamic Law privacy is confined to the concept of physical intrusion whereas nowadays it is possible to invade a person's privacy without physical intrusion of the private sphere.

5.2 The Islamic Law of Evidence and Privacy

The Muslim jurists agree that high standards of testimony in most of the criminal cases are required to punish an offender. For example, in cases of adultery the law requires four witnesses. The stipulation of a testimony by four witnesses in order to prosecute a person who is accused of adultery is a sign of Islamic law's adherence to the protection of privacy since such a stipulation deters those with inquisitive attitudes from violating the privacy of those who may be practicing such unlawful activities in their private environment. When three eyewitnesses testify that adultery had been practiced not only is it insufficient to prosecute the accused, but also the witnesses may be accused of slander.

Privacy in Islamic law enjoys an influential position in terms of its penetration of both criminal and civil legal matters, since it is the ultimate reference as to whether there are any fruits to considering an act illegal or undesirable from a legal point of view. When the law of evidence makes harder trying people who are accused of privacy-related offences, its promotion of privacy becomes all the more significant. Islamic law's promotion of privacy is remarkably beyond the modern man's expectations.

The Prophet discouraged people from confessing to committing shameful acts which have not resulted in infringement on people's rights. The spirit of respect for privacy in this line of thought is emphasized by other traditions. For example, the Prophet has reportedly said, "If you have been embroiled in an embarrassing sin, which God chose not to disclose, do not disclose it yourselves." The Prophet has even turned his face away (twice) from a man who wanted to confess before the Prophet that he committed adultery. After the man insisted on conveying his confession for the third time, the Prophet investigated the possibility that the confessor's mental state or drunkenness may have led him to make his confession. Only after these possibilities were excluded, the punishment was carried out. Some Muslim jurists have relied on this story to argue that people are not encouraged to confess to committing crimes that have not been prosecuted, if the rights of others (such as their property, etc) are not involved. It is clear that such a rule promotes the individual's privacy. However, the Prophet is reported to have insisted that once complaint about a major crime is elevated to the Muslim authorities, no one can stop the prosecution of the criminal.

Another example of the protection of privacy offered in the Islamic law of evidence is that Muslim jurists express their reluctance to accept the testimony of individuals when it is made either for or against a family member or a former family member of their own. Family members, are the ones most acquainted with the details of each other's private life. Although Muslim jurists do not use the language of privacy to justify their reluctance to hear these testimonies, their attitude has definitely led to the enlargement of people's privacy.

One more (rather striking) example of the protection of privacy in the Islamic law of evidence may be discerned from the following: under Hanafi law, if someone confesses (in confidence) to committing a crime in the presence of another and asks the latter not to convey to others the content of her/his confession, the confession witness must refrain from testifying against the confessor. But, what if the person decides to violate the confessor's privacy anyway? Here disagreement arises- some Hanafí jurists call upon the judge to accept the hearing of that testimony and others do not. Thus, according to the first opinion, although the one who promised not to convey the content of the confession was supposed to keep his promise, his privacy-violating testimony may be heard.

According to the other opinion, such a testimony may not be heard. The same disagreement among Hanafí jurists arises in the case where a man denies his debt in public and acknowledges it only when he meets in private settings with his creditor. If the latter allows two persons to attend a private encounter without his party's knowledge and solicits the denier's acknowledgement of the debt, can the judge support the creditor's claim based on the testimony of the secret witnesses? Hanafí jurists have disagreed on this question: some accepted the hearing of the testimony despite the violation of privacy and some rejected it because of the unlawfulness of deception and spying.

Islamic law acknowledges the right to privacy and links it to communication, information, territorial and bodily privacy. However, Islamic Law alone cannot address the challenges that arise from privacy breaches in the ever -changing world of emerging technologies.

6 PRIVACY PROTECTION UNDER SAUDI LEGISLATION

Whilst Saudi Arabia under the Vision 2030 has launched many projects and initiated numerous initiatives to improve the health care service, foreign companies and health organizations in Saudi Arabia are still grappling with legal issues to make use of cloud computing due to the legal vacuum and the absence of legislation as to privacy and data protection (Torry Horris, 2015).

6.1 Ministry of Health Vision e-Health

The Ministry of Health (MoH) under Vision 2030 has developed a business strategy and 5years plan to realize this vision, and has positioned e-Health as a primary transformation agent and enabler (Ministry of Health, 2018). The e-Health strategy supports the primary MoH goals:

To care for patients

To connect providers at all levels of care

To measure the performance of healthcare delivery

To transform healthcare delivery to a consistent world-class standard.

The e-health strategy will benefit the healthcare professionals (doctors, nurses.), who will have access to patients' data at any time, to information that allows them to compare their own practice results and trends against national performance statistics.

It will also benefit the patients by allowing them to access credible health information from any preferred channel (web, SMS, telephone...), receive a faster diagnosis when medical care is needed, reducing time, pressure and confusion when getting services from different locations.

These are some benefits of the Saudi e-health strategy under Vision 2030.

Huge efforts have been made by MoH to improve the health care services, however in terms of laws for privacy and data protection, Saudi Arabia doesn't have a privacy law and data protection.

6.2 Legislation

As of 2018 Saudi Arabia has not passed a comprehensive legislation on privacy or data protection per se, although it has devised a strategic plan for privacy protection. However, currently, there are Laws which may be considered legal instruments in the protection of data.

6.2.1 Constitutional Laws

The Basic Law of Governance no: A/90 dated the 27th Sha'ban 1412H (1 March 1992) which refers to the Constitution of Saudi Arabia provides for the privacy of individuals in article 40. The protection includes privacy of telegraphic, telephonic, postal and other means of communication. It prohibits interception or eavesdropping of private communication except for legal purposes.

Similarly, the Civil Service regulation in article 12 prohibits the civil servants to disclose secret or confidential information acquired while at work. The Constitutional provisions could be applied to protect e-health information of patients in private sector and the public sector employees are bound by the Constitution and Civil Service regulation. These two laws could be easily applied to cover any unlawful use, collection and disclosure of information of e-health patients. In the absence of any relevant legislation, the Saudi judges have discretion to apply Shariaa principles which stipulate that an individual, in case of breach, be compensated for his loss as a result of the disclosure of his personal data by another party (Reda et al., 2012).

Furthermore, there are other specific sector laws which may be used as legal instruments in the protection of data in Saudi Arabia.

6.2.2 Specific-sector Laws

There are certain general available laws that can be extended to protect e-health data privacy and "Data"

under article 1(4) of the Anti-Cyber Crime Law of 2007 (Royal Decree, 2002), is defined as information, commands, message, voices or images which are prepared or have been prepared for use in computers. This definition could include a saved, processed, transmitted or constructed data. If the private information of a person is processed by computers, then this definition could include private data. However, there is no available definition of "personal data" given in any existing legislation though one could define it as any information relating to a living and identifiable individual. Similarly, privacy is not legally defined but could be interpreted as a right associated with the dignity of an individual. Anti-Cyber Crime Law in articles 3-5 penalizes violation of private data which is transmitted via information networks without consent or authorization. Violation of these provisions will warrant a penalty up to SAR 3,000,000 in fine and a maximum of four years' imprisonment. Thus, any personal information including e-health data available in the Cloud will be protected against unauthorized collection, usage or misuse.

The Telecommunications Act issued by the Council of Ministers Resolution No 74 of 05/03/ 1422 H (23 May 2001) and its Bylaws also could be applied in protection of privacy or data privacy. Article 37(7) prohibits telecommunication service providers from intercepting data or calls carried on public telecommunication networks. Article 37(13) criminalizes intentional disclosure of information or content that have been intercepted. The bylaws in article 56(1) state that a service provider shall not disclose information other than users' name address and telephone number without prior consent from the users or if otherwise required by law. It also requires to take all reasonable steps to ensure the confidentiality of users' communication (article 57 (1)).

Article 58 (2) and (3) of the bylaws mandates the operators of telecommunication facilities and networks to respect privacy of users. The bylaw also states that user information shall not be collected without informing the user. It also prohibits collection, usage, maintenance and disclosure of personal information for undisclosed purposes.

Thus if the telecommunication service providers are also providing Cloud services for healthcare facilities or educational service facilities they are expected by law to adhere to privacy and data protection rules under Telecommunications Act and its Bylaws. Any unauthorized use, disclosure and transmission of information will be punishable by this law. This law imposes a fine not exceeding SAR 5,000,000.

In addition, the Electronic Transaction Protection Law (promulgated by Royal Decree No. M/8 of 8 Rabi I 1428H (March 26 2007) also mentions the privacy protection of users of the services of certification service providers. The law in article 1(11) defines "electronic data" as data with electronic features in the form of texts, codes, images, graphics, sounds or any other electronic form, either collective or separate. Article 18(5) requires the certification authority to maintain and ensure that their staff maintains the confidentiality of information obtained in the course of business unless authorized by the certificate holders. This authorization must be either in writing or electronic form. Oral authorization is not considered as authorization under this law. Article 23 (2 -4) states the following as offence: A certificate holder's use of information concerning the applicant, for purposes other than certification without the applicant's consent in a written or electronic form. A certificate holder's disclosure of information accessed by virtue of his work without the certificate holder's consent in a written or electronic form, or as provided for by law. A certification service provider's provision of false or misleading information to the Commission, or misuse of certification services.

In the event the e-health or education cloud service providers or the users obtain certification from a certification authority, any breaches of private information provided in the course of business needs to be kept secret by the certification authority unless authorized. Any abuse will warrant a fine up to SAR 5,000,000 fine and a maximum of 5 years' imprisonment or both. In addition, the Healthcare Professions Practices Regulation requires the health practitioner to protect personal information of patients. This law could be extrapolated to services provided via cloud computing facilities.

Furthermore, the KSA Healthcare Practice Code requires that a health practitioner safeguards the secrets of patients except inter alia where written approval of the relevant patient is obtained. Violators of such confidentiality requirements can be subject to a fine not exceeding 20,000 Saudi Riyals (approximately US$5,333) and other disciplinary penalties such as the suspension of practicing license. Such penalties may be increased based on the severity of the relevant breach or its reoccurrence.

However, Saudi Arabia's data protection and interception laws and implementing regulations are still relatively new and developing. They reflect the Growing global recognition of the importance of control over private data in the digital age. The organization possessing such data should be aware of information where that disclosure result in loss or harm to the individual (Cisco Systems, 2009).

6.2.3 Limitations

Whilst the government of Saudi Arabia is determined to provide best health care facilities and spent billions to upgrade the systems including IT infrastructure, until today Saudi Arabia didn't see any specific provisions on data protection. Thus the Saudi courts are left with considerable discretion to deal with privacy breach complaints and in the absence of a comprehensive legislation on data privacy, the general principles of Sharia law will prevail. In addition to that there is no central place where decisions are continuously indexed, collected and made available for the public. some consider that the lack of a binding precedent system makes the situation more complex (Pearson, 2012).

7 CONCLUSIONS AND RECOMMENDATIONS

Whilst the use of cloud allows providers and more importantly health care delivery organizations the opportunity to focus less on IT management and more on delivering care to the patients (Chikhaoui et al., 2017), Saudi Arabia still continues to have a legislative vacuum in privacy and data protection, leaving the courts under a full discretion as to the application of a specific law in case of data privacy violations.

One cannot ignore that Saudi Arabia is investing generously in the field of healthcare, specifically on the improvement of health care and the use of technology to provide better services. Moreover, debates and researches are conducted to introduce cloud computing in the health sector and steps have already been taken.

The Ministry of Health is aware that the improvement of health care services and the ever growing medical data requires expansion of current computational and storage capacities. In order to meet the needs of medical departments, health care facilities must continuously improve the level of modern system by using advanced science and technology innovation (Chikhaoui et al., 2017).

The updating and maintenance of IT systems in healthcare facilities is neither cost efficient nor effective. Cloud computing is the only technology that mitigates the continuous need to invest in IT infrastructure, by providing access to computing resources, applications, and services on a 'per use' model, which dramatically brings down the cost and simplifies the adoption of technology. Several EMR vendors are offering their solutions as a cloud-based offering, providing an alternative approach to help hospitals better manage the otherwise massive capital IT investments that would be needed to support EMR implementations (Chikhaoui et al., 2017).

However, there is an ongoing debate within healthcare as to the viability of cloud-based solutions given the need for patient privacy and sensitive personal information (Anand et al., 2014).

Privacy, security of information and confidentiality are the issues raised in Saudi Arabia as to moving to the cloud in the health sector. The Cloud computing paradigm is still relatively young in terms of maturity and adoption.

Before moving completely to the use of this new technology, the risk should be assessed as to the trust in the Cloud Service provider for the security of sensitive information of health and the consumer should be fully aware in order to avoid any problem as to the violation of data protection. In addition, a comprehensive law on privacy and data protection should be implemented to protect the safety of individuals' personal data against any misuse or theft of data.

The availability of a comprehensive legislation on data privacy will definitely complement the government's effort to have an international recognized heath sector.

ACKNOWLEDGEMENTS

The author acknowledges the support of Prince Sultan University in doing research and is grateful to Microsoft for funding previous research in similar topics.

REFERENCES

Chandra, Adesh. (2013) 'Privacy Issues and Measurement in Cloud Computing: A Review', *International Journal of Advanced Research in Computer Science*, Vol 4, No. 4.

Asad, Muhammad. (2008) *The Message of Qur'an.* California: The Book Foundation.

Bin Asha'th, Suliman. (2008) *Sunan Abu Dawud,* Book 8, Hadith 1480. Riyadh: Darussalam Publishers.

Muhammad, Abdulkader. (2011) 'Information Technology (IT) Ethics in the light of Islam', *International Islamic University Chittagong*, Vol. 9, p243 – 260.

Rehman, Hafiz Aziz. (2017) 'Right to privacy: A comparative perspective in law and Shariah', *Acta Islamica University of Islamabad*, Vol. 5, p. 25.

Torry Horris Business Solutions. (2015) Cyber Security and Data Privacy Law in Saudi Arabia.

Gupta, Vishal. (2011) 'Cloud Computing in Healthcare', Express Healthcare. Available at: http://archivehealthcare.expressbpd.com/201109/itathealthcare04.shtml.

Ministry of Health. (2018) 'National e-Health Strategy Vision 2030'. Available at: https://www.moh.gov.sa/en/Ministry/nehs/Pages/default.aspx.

Reda, Eyad and Alsheikh, Turki. (2012) 'Data protection in Saudi Arabia', Thomson Reuters.

Royal Decree. (2007) 'Anti-Cyber Crime Law', No. M/17 8 Rabi I 1428/ 26.

Cisco Systems. (2009) 'Cloud Computing in Healthcare'. Available at: https://www.cisco.com/c/en_in/about/knowledge-network/cloud-computing.html

Pearson, Siani. (2012). 'Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing' p.3-42, HP Laboratories. Available at: https://pdfs.semanticscholar.org/59c5/cb96e6160d0b076286f4052f310c3bba7f19.pdf.

Chikhaoui, Emna, & Sarabeddine, Jawahitha, & Parveen, Rehana. (2017) 'Privacy and Security Issues in The Use of Clouds in E-Health in The Kingdom of Saudi Arabia', *IBIMA Publishing*, Vol. 2017. Available at: https://ibimapublishing.com/articles/CIBIMA/2017/369309/369309.pdf

Anand, DR. S.K. Srivatsa, (2014) 'An Implementation of Health Care Industry Through Cloud Computing Technology', *International Journal of Emerging Technologies in Computational and Applied Sciences*, p.332-333. Available at: http://iasir.net/IJETCASpapers/NCRICA.pdf.