

RIGHT TO PRIVACY IN CYBER SPACE - A STUDY WITH REFERENCE TO PRIVACY OF PATIENTS IN HEALTH CARE INFORMATION K.S.A.

Dr Maha Abdu Othman, Dept of Dentistry, Jazan University, KSA, Dr Saleena K B, Dept of law , Jazan University, KSA

ABSTRACT

The research is about the challenges of internet on privacy in general and privacy of health care data in the context of Saudi Arabia in particular.

Key Words: Cyber space, right to privacy, data protection

I. INTRODUCTION

The Kingdom of Saudi Arabia stands upright among its own type due to the utmost importance it provides to the cultural and social values of the country, basically the Islamic principles. The country's vigorous economic profile and encouraging government policies have enabled Saudi Arabia to reach high ranks of the top countries in the world. This growth is due to the large quantities of oil deposits in the country. It is really favorable in terms of ease of doing business also. Prior to the unearthing of oil, kingdom was old-fashioned, secluded and poor. The life was very pragmatic and very much backward. During this period, healthcare system was not well established. They relied on traditional practices and medicines. But during the beginning of 19th century they were able to establish a National Health Department¹. This is earmarked as the beginning of modernization in health care system. This department began to supervise the health care of the country.

The intrusion of use of internet was slow paced in the country in comparison with other countries of the world. But it acquired greater momentum after 1999. Still the country remains successful in regulating the inner and outer flow of internet through various legal measures. Various problems are faced by the country in the access, regulation and use of data collected² through computer. Data³ handling is one of the major threat. Anonymity and easiness of handling data through internet always remains greater concern of government and citizens. This is particularly matter of Security for the nation and protection of privacy of the providers of data⁴. The rapid technological progress outweighs the laws which are slow growing. Provision of a

Secure digital environment is one of the national strategies adopted under country's vision 2030⁵. But there is a great challenge before the government how to balance the security of cyber space and informational privacy of medical records. These medical records have several benefits. There is a reduction in costs for hospitals. It facilitates easy review of medical errors and improves the quality of care with greater transparency about the patients for healthcare providers. Thus the national healthcare system achieves greater efficiency. These records have some secondary uses also. The ready availability to mine and process large volumes of medical data can be helpful for the purpose of research and analysis. Saudi government need to serve the needs of advance health care of 28.2 million citizens also. To achieve the vision and mission of 2030 digitalization of health care data is a justified priority, so that the precious time of health care professionals can be used with due diligence for the care of people. Currently the country is on half way in the adoption of electronic medical records. There is advanced technologies in major cities and hand written records in rural clinics. But it is sure that the future belongs to paperless clinical documentation. In order to be acceptable it must be cost effective as well as giving adequate protection to the data furnished.

Therefore the issue of privacy is very sensitive and the nations face number of problems while dealing with this issue. The concept of privacy is a relative term which acquires different colours according to the context in which it is used. Privacy can be divided into separate but related concepts such as informational privacy, bodily privacy, privacy of communications and territorial privacy. The personal data stored and used create great threat towards all forms of privacy above mentioned. The personal data are any information that directly or indirectly allows the identification of individuals. It refers to and may include contact data such as name, mailing address, telephone number, credit information, medical records covering medical and genetic information of the patients, government or public records containing tax identification number or the individual's social security number. But there is unanimity among various nations regarding the medical records as they directly relates to the life and dignity of every patient.

The information or data provided by patients are highly protected under the broad principle of shari'ah⁶, that disclosure of secretes is prohibited except where the owner

¹ Refer <file:///F:/saudi%20research/saudi%20health%20care%20system.pdf>. Visited on 10-02-2019.

² Computer database refers to a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network

³ The expression data is very wide in ambit and scope. It includes personal aspects of individuals as well as commercial aspects. The former is protected in the form of privacy rights and the latter as proprietary rights.

⁴ Data referred here after relates to the digitalized medical records alone.

⁵ Refer <file:///F:/saudi%20research/Data-Protection-in-the-Kingdom-of-Saudi-Arabia.pdf>. (Visited on 13-01-2019)

⁶ Refer <file:///F:/saudi%20research/privay%20in%20gulf.pdf>, visited on 1-03-2019

of relevant secret agrees to such disclosure or if it is necessary for public interest. Based on this principle patients data is protected under KSA Health Practice Code, 2005⁷. This casts duty on the health practitioners to safeguard the secrets of patients which he comes across⁸. It can be revealed only if there is a written approval from the required patient. This code provides severe punishment to violating practitioners⁹. But the problem of data protection in the field of health information has bypassed what is envisaged under this code¹⁰.

This arouses the curiosity of the whole nation as to who is primarily responsible for the privacy of digital information of patients? How do they protect privacy in practice? How do the privacy rights are balanced with other interests involved? How this issue is dealt in other jurisdictions especially in U.S. and U.K. this article also deals about how accesses to these records are regulated. What are the technological measures to be adopted to protect the data? It is also necessary to consider the role of law in promoting greater information privacy in general and cyber space in particular.

II. DATA PROTECTION CHALLENGES AND PRIVACY ON INTERNET

An advance in computer technology has made greater advances in the life of man including the information that can be stored retrieved, accessed and collected instantaneously. Information centralization results in the flow of information in one tap of a button. These are cross matched data's which can be used even to predict the personal choices, behavior of an individual etc.

This has greater impacts on the life of man. Revelation of privacy of man is one among the crimes committed through the internet and technology. This can even impair the life of man. This will badly effect the society and social relations. Privacy of data involves control over one's own identity, information regarding the personality, prediction of behavior, life style and in medical data even the private life of a person will be revealed. This can also include the financial affairs also. Unnecessary intrusion by anyone without the express or implied consent of the person concerned is clear violation of the recognized right of privacy under any jurisdiction.

⁷ Royal decree no. M/59, 4-11-1426 H, <https://www.boe.gov.sa/ViewSystemDetails.aspx?lang=en&SystemID=164&VersionID=178> accessed on 01-03-2019.

⁸ Article 5, Art 7 (b) and art. 21 deals with various aspects of confidentiality. Article 21 is the main article which states that a health care professional shall maintain the confidentiality of information obtained in the course of his practice and may not disclose it except in the circumstances specified.

Article 24 mentions the mutual trust is the ingredient of this profession.

⁹ *Id.* at article 28 and 30.

¹⁰ <http://saudigazette.com.sa/article/560119>, snap chat doctor violates patient's confidentiality.

This outcome from the influx of technology was predicted even centuries before. In *Olmstead v. United States*¹¹, Justice Brandeis opined that, growth of communication technologies have full filled the century old prophesy¹². He added that private lives of every man are now exposed by electronic retrieval and publication of personal information. According to him for civilized man privacy¹³ is the most comprehensive and valuable right. This should be protected from unnecessary intrusion from the governmental and non-governmental entities.

In many countries right to privacy is considered as fundamental right¹⁴. But this is not an absolute one¹⁵. Thus the earlier view of right to privacy acquired a changed meaning of controlling information pertaining to an individual. Thus the informational privacy is an emerging facet of right to privacy. Even though the informational privacy is of great concern for nations increasing amounts of personal information are collected and revealed

¹¹ The case, *Olmstead V U.S.* 227 US 438 (1928), with Justice Brandies dissenting, available at <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=277&invol=438>, visited on 25th Jan.2019.

¹²A famous legal article titled "The Right to Privacy" written by Samuel Warren and Louis Brandeis and published by the Harvard Law Review in 1890. In this article authors had shown concern for privacy more than a century ago about how new technologies could affect privacy. They wrote: "recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'. For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago, directly involved the consideration of the right of circulating portraits; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration." The article Right to Privacy by the authors is available at <http://freedomlaw.com/Brandeis.htm>, visited 25th Jan.2019.

¹³ He refers privacy as "the right to be let alone".

¹⁴ Supreme Court of India in *Justice K.S. Puttuswamy v. Union of India*, 24th August 2017 held that right to privacy to be a fundamental right.

¹⁵ It can be restricted by law, in pursuit of a legitimate state interest, proportional to the object and the needs sought to be full filled by the restricting law.

electronically in the name of greater convenience. This has blurred the demarcation that earlier existed with regard to public and private¹⁶ realms of information. But the policy makers are eyeing at not what technology makes possible, but at the core values the Constitution enshrines. It reveals that the principles relating to privacy must be invariable despite the accidents of technology. Thus there is an irony that exists now is 'the very technology that simplifies our lives simultaneously complicates our legal analysis of this most fundamental of concepts'.

III. WHY HEALTH CARE INFORMATION TURNS TO BE AN ISSUE UNDER CYBER SPACE?

The vast changes in technology and business practices have made the individual data a lucrative commodity¹⁷ apart from easing the jobs of data collection and storage. Personal information collected in the hospitals have been commoditized by commercial entities without due consideration¹⁸ of right to privacy. The most important concept of privacy in health care is confidentiality¹⁹. Access to information is another important factor. Access to information is provided through Medical Records²⁰. Medical Records can be defined as a chronological written account of a patient's examination and treatment that includes the patient's medical history and complaints, the physician's physical findings, the results of diagnostic tests and procedures and medications and therapeutic procedures. If a patient's protected health information is stolen, it can translate into a cybercrime. This is because protected health information can be in digital form.²¹ This is significant because the data that is contained within a patient's protected health information includes numerous personal facts about the patient. These facts can include the medical information, past health problems, present health ailments and billing information

¹⁶ Priscilla M. Regan, *Privacy, Technology And Public Policy*, University of North Carolina Press (September 1995) at p 2 .

¹⁷ Alok Prasanna Kumar, "the Puttuswamy Judgement Exploring Privacy within and without", *Economic and Political Weekly*, Vol. 52, Issue no, 51, Del. 2017, pp.34-35.

¹⁸ In *Mr. X v. Hospital Z*, (1998) 8 SCC 296. Indian Supreme Court had justified the intrusion to privacy for prevention of crime, disorder or protection of health or morals or protection of rights and freedoms of others.

¹⁹ A physician's duty of confidentiality finds expression in the Hippocratic Oath. It requires health care providers to keep a patients personal health information private unless consent to release the information is provided by patient. See Jessica De Board, et al., "Confidentiality, Ethics in Medicine", University of Washington School of Medicine, <https://depts.washington.edu/bioethics/topics/confiden.html> (accessed on 17-07-2018)

²⁰ See www.dictionary.com/browse/medical-record (accessed on 15/05/2018)

²¹ (Kim & Solomon, 2012, p. 442).

Privacy violations in the health sector that stem from policy²² and implementation gaps. These violations include disclosure of personal health information to third parties without consent, inadequate notification to a patient of a data breach, unlimited or unnecessary collection of personal health data, collection of personal health data that is not accurate or relevant, the purpose of collecting data is not specified, refusal to provide medical records upon request by client, provision of personal health data to public health, research and commercial uses without identification of data and improper security standards storage and disposal. Apart from that Healthcare records are an extremely attractive target for cyber criminals. These contain various bits of sensitive information such as names, addresses, payment details and so on, in one place. It can lead to identity theft²³. Therefore the disclosure of personal health information has the potential to be embarrassing, stigmatizing or discriminatory. But in reality most of the people believe that the notion of patient privacy is usually limited to the rights of individuals regarding their personal health information being used or disclosed without their consent.

Professional's discourse about privacy reveal show new technologies and laws challenge existing practices of information control within and between professional groups in healthcare, with implications not only for patient privacy but also for the role of information control in professions more generally.

Personal privacy and dignity of an individual while being examined clinically by a health professional is also an upcoming issue in many parts of the country as the health care professionals are mostly hired from various cultures and countries.

Thus the privacy violations in health care data would result in human rights violations, property rights violations, defamation, breach of trust and confidence on the basic policies followed by the nation, unnecessary economic exploitation, breach of fiduciary relationship between health care professionals and patients.

IV. PRIVACY CHALLENGES IN HEALTH CARE APPROACH OF SAUDI ARABIA

Health care industry shows a steady growth in Saudi Arabia due to various factors. They are rapidly growing population, increasing per capita income and a high incidence of lifestyle-related diseases. Along with these supporting factors such as rising life expectancies and ambitious medical infrastructure projects add momentum to this growth. Health care is the prime concern of the nation and mostly government funded²⁴.

²² Policy of each nation is laid down in the law of the land in most of the country's, constitution and in KSA "The holy Quran".

²³ The health industry endured 122 breaches as on 10th May 2016, which compromised 4,025,085 healthcare records. [http://E:/saudi%20research/Cyber-Security-in-Healthcare-04%20\(1\).pdf](http://E:/saudi%20research/Cyber-Security-in-Healthcare-04%20(1).pdf) accessed on 20-02-2019.

²⁴ As per the available data, the government spend on healthcare in Saudi Arabia, accounted for 65.8% in 2012, according to the World Health

Along with the implementation of digitalization of medical records²⁵ country have invented various measures²⁶ to deal with the cyber security. The Basic Law²⁷ of Saudi Arabia contains language that calls for freedom of speech. The Law of Print and Press, 2000 also addresses freedom related to expressions. These are oriented towards restrictions than protections. The Anti-cybercrime law, 2007 provides stringent punishments to the violators²⁸ and persons who involve in data theft. The Health Practice Code, 2005 also brings out strong measures for the privacy and data protection for the patients. The anti- cybercrime law enacted by Royal Decree No. M/17 of March 26, 2007, article 3(5) deals with law of defamation and infliction of damage upon others through use of Digital Technologies. This offence is punishable with imprisonment and fine. Article 6 of the Act deals about invasion over privacy through transmissions under the mediums of information technologies. This crime is also made punishable with imprisonment and fine. Along with this Saudi Health Care Regulation, makes the health practioners duty bound to protect the confidentiality of patient information unless the patient has consented the disclosure of that information in writing. Apart from this Sector specific laws also regulates the transfer and transmission of data base such as Banking Information regulation requires the permission of Saudi Arabia Monetary Agency in order to complete the transfer. The approval of Saudi Food and Drugs Authority is required to transfer certain health related information outside Saudi Arabia. Article of the Basic Law of Governance guarantees the privacy of postal, telephonic and other communications. Finally the international initiatives to protect the data privacy also affects the KSA.

Despite these measures country finds highest malware detections in the region. Thus every industrial experts including health care are of the opinion that the cyber security remains exceptionally important challenge of the region. Healthcare is more and more targeted by cyber criminals. There is sluggishness from the part of the industry to react towards the breaches of patient health information. For cyber criminals, the healthcare records extremely attractive as these contain various bits of vulnerable²⁹

information. Every bit of such information can fetch a high price on the underground markets of the dark web. The healthcare industry is far behind the cyber preparedness required for the protection of data. There is an increased risk due to the uniqueness and richness of the information that the doctors, hospitals, health plans and other health care providers handle. Apart from the data theft there is also a possibility of medical insurance fraud, apart from typical financial fraud.

V. ROLE OF INFORMED CONSENT AND REGULATION OF DATA USE

Informed consent is defined as "...an autonomous act by a patient or research subject to expressly permit a professional person to perform a medical action on the patient or to include a person in a research project". The main argument is whether the informed consent, as it advocated in the western culture, is suitable for KSA³⁰. The western concept of informed consent is based on secular notions and the Saudi concept is rooted on the Sharia'h law and more religious. Studies reveal that both notions are similar with regard to the respect for privacy. This includes; that every patient has the right to respect, dignity, integrity, safety, protection, privacy, and moral, cultural, and religious values with appropriate measures for disease prevention and health care. In addition to these, everyone has the right to receive information about health services and how best to use them, the right to receive information about health status on request, the right to know possibilities to have other opinions, the right to refuse treatment, the right to complain, and the right of getting informed consent, patients' autonomy, privacy and confidentiality³¹.

Under common law all competent adults can consent to and refuse medical treatment. If consent is not established, there may be legal consequences for health professionals³². At the international level also the right to respect for his or her physical and mental integrity on an equal basis with others is adopted by various instruments³³. Where the patient is not in a position to make such informed decision assistance can be sought from state or next friend.

In Saudi Arabia this issue is governed by 'Manual Guide for Medical Practioners'. This code provides guidance to medical practioners in Saudi. This clearly states the rights of

Organisation (WHO). Saudi Arabia also spent around \$35.9 billion on healthcare provision in 2013, which amounted to 4.8% of GDP. Total healthcare spending is projected to rise by an average of 6.2% per year between 2014 and 2018, to an estimated \$48.3 billion. See [file:///F:/saudi%20research/Cyber-Security-in-Healthcare-04%20\(1\).pdf](file:///F:/saudi%20research/Cyber-Security-in-Healthcare-04%20(1).pdf) (Visited on 10-02-2019)

²⁵ Towards national e-health. Saudi e-health conference, 17–19 March 2008. Riyadh, Saudi Association for Health Informatics, 2008 (<http://www.saudiehealth.org/2008/>, accessed 28 June 2011).

²⁶ See file:///F:/saudi%20research/FOTN%202017_Saudi%20Arabia.pdf. (visited on 12-02-2019)

²⁷ *Supra note 6*

²⁸ This Act criminalizes "producing something that harms public order, religious values, public morals, the sanctity of private life, or authoring, sending, or storing it via an information network," and imposes penalties of up to five years in prison and a fine of up to SAR three million (US\$800,000).

²⁹ Vulnerable data includes clinical information such as diagnoses and ordered tests. These are highly privileged data that nobody would want to fall into the wrong hands.

³⁰ Adlan A.A. (2013) Informed Consent in Saudi Arabia. In: Beran R. (eds) Legal and Forensic Medicine. Springer, Berlin, Heidelberg

³¹ See <http://www.moh.gov.sa/en/HealthAwareness/EducationalContent/HealthTips/Pages/Tips-2011-1-29-001.aspx>, accessed on 13.09.2018.

³² Under the law of trespass, patients have a right not be subjected to an invasive procedure without consent or other lawful justification, such as an emergency or necessity.

³³ *Rogers v. Whitaker* (1992) 175 CLR 479.

See also, *Secretary, Department of Health and Community Services v JWB and SMB (Marion's case)* (1992) 175 CLR 218.

See also In March 1994, Amsterdam held the European Consultation on the rights of patients under the auspices of the WHO Regional Office for Europe. The purpose was to define principles and strategies for promoting the rights of patients within the context of the health care in most countries

patients³⁴ to give consent to medical intervention as well as confidentiality of his or her medical information. The definition part of the rights and responsibilities of patients says about a declaration form³⁵. Under these document patient is entitled to privacy and confidentiality³⁶.

VI. WAYS POSSIBLE

The reported incidents in the area of privacy violations are at an increasing pace. This needs positive intervention through the advanced technologies apart from the legislations with stringent penalties and punishments. One of the possible solution can be digital transformation of medical data. Digital dictation solution with speech recognition can also be adopted by country to encounter the problem. Clinical speech recognition supports health care professionals allows the medical professionals to save their time and reduce their burden either of dictation or manual entering the data. By this method computer can capture the narrative patient data. Cloud computing and mobility is another solution put forward worldwide. Cloud technology is in formative stages which require a centralized administration of data, which is disseminated and accessed from any hospital according to the requirement of the patient where he wishes to seek treatment.

Development of health policy in shaping and sharing of health information is necessary with stringent health information privacy policies.

³⁴

<https://www.moh.gov.sa/en/HealthAwareness/EducationalContent/HealthTips/Pages/Tips-2011-1-29-001.aspx>, visited on 4-03-2109.

Under this, Ministry of Health provides all health services in its facilities to patients without any discrimination. In addition, it acknowledges the rights of patients and their families during their treatment in its facility and expects them to fulfill the responsibilities assigned to them.

³⁵ *Id.* at definition part

Declaration Form:

Declaration form is a form that is not valid unless it's filled out by the patient or his/her legal guardian. That is to start conducting the requested procedure, where the signature is considered an approval of the information contained in the declaration form.

³⁶ *Supra* n. 42 at

3/ Privacy and Confidentiality: The patient and his/her family are entitle to:

Discuss the treatment with the patient or his/her legal guardian confidentiality.

Cover the patient private parts unless a medically urgent situation arose.

Maintain the confidentiality of the patient's information, diagnosis, tests, treatment and medical records. That is unless the patient or legal guardian grants the permission to release them - unless it's legally needed.

Refuse to see anyone not concerned with providing the health service, including visitors.

Patient medical record is accessible only to:

The medical team caring for the patient.

The quality management program team.

The health facility research team.

People with a written authorization of the patient, legal guardian or legal authorities.

Provide the patient with appropriate outfits and necessary personal kit.

Have separated male and female waiting areas.

Transfer the patient to a private examination room if his room was not suitable for examination.

Ensure the presence of someone of the same sex as the patient in the examination room.

Ensure that the patient doesn't stay in the examination room more than needed.

VII. CONCLUSION

Privacy in the context of health care information is “control over personal information and personhood”. From the Islamic point of view it is a permanent value that touches upon all aspects of behavior. Islam recognizes this as the fundamental human right. Primarily an individual is responsible for achieving the level of privacy they need. It can be achieved only when an individual is able to make a personal balance between withdrawal and disclosure to a group. It is the claim of respective persons to determine for themselves when, how and to what extent information about him/her is communicated to others. Every information such as identity, trends, tendencies, banking and financial dealings are linked to person's private life. Thus a person is identified by definable information.

Every citizen or any person who seeks health care in KSA expects that their data to be secure, accessible only by authorized people. When government uses this citizens expect that their data will be kept at all times in a secure place with high quality.

Information technology infrastructure with regular maintenance is the most important requirement in this regard. Use of new and novel technologies to secure their data is advisable. Irrespective of the nationality the data should be secure.