



# INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 6.078

(Volume 6, Issue 3)

Available online at: [www.ijariit.com](http://www.ijariit.com)

## Privacy policies of health care companies

Akshay Mittal

[amittal3061@ucumberlands.edu](mailto:amittal3061@ucumberlands.edu)

University of the Cumberland, Williamsburg, Kentucky

### ABSTRACT

*The need for and importance of privacy policies across the healthcare continuum is based on the basic and fundamental human rights. International laws and regulations are linked to the physician's oath of confidentiality and secrecy. The general medical council provides formwork for healthcare to design the privacy policy to protect confidentiality (Abi, 2017). Various fields across healthcare continue like a chronic disease which might make a patient terminally ill for e.g. Human immune deficiency virus (HIV), types of cancers make patients vulnerable and depressed to a great dept. Humans are social animals and are psychologically affected by treatment. Studies are shown that the placebo effect at patients who are terminally ill has given them a chance to be more psychologically fir and healthier. The second example is international surrogacy laws, confidentiality and privacy policies are of utmost legal importance determining the paternity of the child. Confidentiality and privacy policies are made and communicated to all stakeholders including staff and patients to ensure correct implementation and full protection of patient's data. According to the federal of the country, every organization needs to maintain privacy in policies. In an age where technology is overpowering the healthcare industry and cybersecurity threat is always looming above the head, there is a need to develop and implement more stringent privacy policies. Confidentiality and privacy policies must be communicated to the end-users so as to ensure their consent for the treatment and to boost their confidence, their data, and their treatment. These data must remain confidential at all costs. Confidentiality must be maintained while it is processing. The data processing involves creating, storing, and sharing (Chen, 2016).*

**Keywords**— Privacy, Policy, Data, Security, Healthcare, Cloud Computing, Bigdata

### 1. INTRODUCTION

The privacy policy can be defined as a privacy statement available on the organization's online portal to ensure the safety of the data stored with the organization. Privacy and patient confidentiality are some of the key elements and components of the WHO medical negligence law. The role of the privacy policy is to ensure and communicate the privacy laws to the patients. As per the WHO charter of patient's rights and responsibilities, it is their right to know the patients' privacy (WHO, N.D). The privacy is also linked to the patient's consent policy. The end-user has the authority to give consent to the organization to use his data and diagnosis to medical research as applicable. Privacy and confidentiality policies are also linked with medical ethics laws and medical ethics policies.

The privacy laws are so stringent that healthcare professionals are trained even on talking about the patient out of their office hours and in public places. To maintain the trust of the patient's the organizations like Zuleqa hospital, and the Thumbay hospital mentions the policy on their e-portal to making the patients aware of the benefits and the challenges to secure the data. The responsibility of the data protection starts from the physician to the healthcare professionals involved in the treatment including the nurses, dietitians, medical coders, medical record keepers, etc including the IT and the administration of the hospital. The Canadian accreditation ACI ensures that the non-medical staff is aware of all the laws regarding the data protection of the patients. The international accreditation standards like the joint commission international, the accreditation Canada, the ISO standards all speak about confidentiality and privacy as components of their standards. An increase in data breaches is experienced with the growth in technology and advancement in the healthcare industry. The management needs to implement privacy policies to protect the information of patients. The confidentiality is not absolute, it is a legal and ethical duty of the medical professionals and is vital for the organization to maintain the privacy (Abi, 2017).

### 2. LITERATURE REVIEW

The doctors or the medical professionals write the prescription to the patients who are now stored with the organization with a unique identification number given to the patient. This facility is to reduce the physical data and enhance accessibility. In one of

the articles, we have seen how the author discussed the removal of limitations to the accessibility of the patient's previous data with the e-portals (Matthan, 2018). Doctors have started writing investigations, follow-ups, medicines, and procedures that are all stored online and can be easily used across the healthcare centers with the patient unique ID. Have all the required components starting from patient identification to patients' nutrition, counseling, admission, treatment and follow up so that all the data is entered in a timely and more secure manner. The advantages of the online system are data confidentiality, proper usage of hospital space, authorized access for staff, and easy retrieval by the use of healthcare numbers (Glenn, 2018).

The challenges faced and the threats that are been faced from the HIMS are data migration from physical records to online new records. End-users adaptability and the use of technology was observed as the challenge. This was also known as the July curve. The greatest threat is the cybersecurity for any data. The technological breakdown of the machine and servers leading to the complete health of the healthcare services is also a threat. The risk of losing data gives sleepiness night to the management. The time consumed for healthcare professionals to rebuild the data is also a threat. The other risks involve legal risk, innovation, compliance, and growth (Thora, 2017).

A unique patient identification number is given to a patient to retrieve his or her information at any point of retrieval within the healthcare organization in a country. The UAE has started working on it on a local level including the pharmacy, labs, outpatient department and other departments of the industry reducing the waiting time of the patients and influencing the conditions of the healthcare professionals. The interaction of IT with healthcare has given new frontiers for better treatment including better diagnosis and better image qualities using technology. The use of technology example using telehealth has managed to provide healthcare services to remote parts of the world thus saving the lives of human beings where even the physical doctor is not present.

The previous privacy policies only limited to the physical files leaving difficulty of the data privacy stored online. The organizations had the privacy policy written but it was not communicated to the end-users. The new recent policies made sure the organization's make it available publicly on their portal/website that is visible and accessible to every user who visits the site. IT and healthcare came together to provide security to the data and enhance the protection, control access with authorization, and secure transmission (Hsu, et. al., 2013).

In order to protect the confidentiality and privacy of the patient's information, the doctors practicing in the UK are asked to include the privacy policy as per the facts guidelines provided to them by the laws and compliances. Patient's consent, the importance of confidentiality, disclosure of patients' information as per law, and disclosure of information by the doctor as per the requirement of the statute are the 5 facts that need to be considered by the doctors (Abi, 2017).

We have experienced growth in the implementation of digitalization and information technology in the healthcare industry. The clouds and cloudlet technology are getting popular with wearable devices. It has enhanced the services and privacy of the patients by processing the data for better results. Data creation, data storage, and data sharing are all part of the data processing of the patient's information. The shift on cloud involved many difficulties for the management like protection from intruders which was solved later by developing and intrusion detection system (IDS) for protection of data (Chen, 2016).

### **3. RESEARCH METHODOLOGY**

The healthcare organizations collect the information of the patients with the aim of storing it and providing the services. It was observed that the physicians write down the prescriptions, medicines, procedures, and the health condition of the patient which is now stored online with the help of the organization's applications such as HMIS. This data needs to be secured as it is confidential. There is a risk of data being hacked for research and studies. The hackers may also target the data to steal the information and blackmail the patients and the organization. Many such cases have been reported lately. To avoid such incidents the healthcare is now started transmitting their data in the encryption form instead of the readable form (Chen, 2016).

The security policies of Thumbay hospital, Zulekha hospital, and the American Hospital Association are designed as per the guidelines provided by the JCI. The medical council also provided the framework for designing and implementing the privacy policy in the organization's portal to secure the data (Abi, 2017).

With a new project at the Zulekha hospital, the communication system was upgraded and implemented as "Avaya aura". It is the latest communication enhancement project providing a contact center as a solution to communication hurdles in security boundaries. In the process, Zulekha hospital developed and deployed a wide range of software and hardware-based on Avaya Aura to deliver highly scalable, resilient, and increased availability to their infrastructure. The hospital staff can now utilize the hardware for better customer engagement avoiding long queues and waiting time enhancing their customer relationship management. As per the documents, the hospital focuses more on customer satisfaction when compared to the return of investments (Shams, 2016).

### **4. RESULTS**

The healthcare companies need privacy policy to be available publicly to protect the information of the patients stored with them and to build trust. This privacy policy is presented separately on the online or e-portals of the hospitals. These policies helped them to minimize court cases. Healthcare processing involves sharing critical data. Traditionally this data used to be moved to clouds with the sensitive information still present in the readable form creating communication hurdles. The development and implementation of cloudlets and IDS enhanced privacy and protected the organization from malicious attacks as they are shared and transmitted in the encrypted form. The organizations now choose the models wisely or create their own models for data

sharing as the new rules allow the patients to access their medical data on a broader way with MyHealthEData. The benefit of this is that it can enhance the medical and healthcare services by increasing the flexibility and sharing information via applications and online services (Glenn, 2018).

This paper showed the importance of presenting the healthcare's privacy policy on the e-portal separately and implementation of new technologies like cloud computing and cloudlets for minimizing the risk, eliminating the communication hurdles and making the data easily available throughout the healthcare industry. The function of the cloudlet is to increase privacy protection, data sharing, and intrusion detection (Chen, 2016). This is made possible for the patients to connect with the Medical services and the medicare beneficiaries and the insurance claims easily. The Zulekha hospital for the ease of the patient's implemented the new method of communication via social media platforms like WhatsApp. The patients can book an appointment via the given contact number on the website. It is a secure way of communication and can even be used for sharing the diagnosis reports. The confidentiality is maintained as per the policy designed and presented by the organization.

## **5. DISCUSSION**

Every healthcare organization like Zuleqa and Thumbay hospital collects private and personal data of their patients to provide services and enhance their accuracy. Hence, the privacy policy is a must in such giant organizations. The organization uses technology and advancements to increase the accuracy and flexibility of data sharing. The users are guided on how to choose trusted models and trusted suppliers for those who want to move their data on clouds. Also, the points are covered on how to use the new initiative MyHealthEdata announced by the administration of Trump gives better access to the patient's electronic health record and insurance claim information. With the development of information technology and computer science, big data can be introduced to healthcare services and research. As the data increases, the need for protection also increases. The organization needs to maintain a strong authorization system to ensure the safety of the patient's information confidentiality (Glenn, 2018).

A framework was considered that has value for the patient's privacy as well as the public health goals. It is noted that were no federal laws to protect the privacy of the people's medical information stored with healthcare before the HIPPA enactment. The new enactments in HIPPA privacy law enforced the entire healthcare to meet their guidelines (Goldman, 1998). In these modern healthcare organizations, the obstacle to get access to the past medical record is removed by implementing digital technologies that overlay relevant data of the patient's medical history so that they can compare it and come up with better diagnostic results. This small fraction of technologies allows the doctor to make an accurate diagnosis (Matthan, 2018).

## **6. CONCLUSION**

It can be concluded that this privacy policy in healthcare helps the organization to ensure safety in the process to obtain the accuracy of the patient's data. The implementation of privacy in policy reduces the number of court cases. After implementing tools for ensuring patient privacy and confidentiality it has been observed that the court cases of the organization were decreasing (Abi, 2017).

The JCI has provided a framework and guidelines for the hospitals to design the policies. This privacy in policy has increased the transparency and helps to build trust between the patients and the healthcare service provider. With the growth in technology and digitalization, it was made possible to make the past reports available to access anywhere increasing the accuracy in diagnosis. The reports of the patients are now stored online on clouds and the organization's network accessible with a provided access id. The access ID and password are provided for authentication and authorization to protect data breaches as the information is sensitive. The portals have a huge potential for growth and are widely accepted. In some countries, it is now mandatory to have an online portal or website on which the organization must have all the policies and information about the organization for easy access and contact flexibility.

The organizations collect the information of the patients for prescription, test reports, and another diagnosis which is stored with them. The need is to secure the collected data which includes the name of the patient, age, health condition, postal address, and other bank or insurance details. The fear of breach of data is minimized with the implementation of these policies. Thus, the organization's like Zulekha hospital, John Hopkins, and Thumbay hospital made sure that the privacy policy is available on the website and is presented separately from other terms and conditions to highlight it.

## **7. REFERENCES**

- [1] Abi, R. (2017). 5 facts about patient confidentiality. Retrieved from <https://www.bmj.com/content/356/bmj.j636>
- [2] American hospital association. (2014). Privacy policy. Retrieved from <https://www.aha.org/2017-12-11-privacy-policy>
- [3] Chen, M., Qian, Y., Chen, J., Hwang, K., Moo, S. (2016). Privacy protection and intrusion avoidance for cloudlet-based medical data science. Retrieved from <https://ieeexplore.ieee.org/abstract/document/7590019/keywords#keywords>
- [4] Federal decree-law on Medical liability. (2016). Retrieved from [https://www.dha.gov.ae/Asset%20Library/MarketingAssets/20180611/\(E\)%20Federal%20Decree%20no.%204%20of%202016.pdf](https://www.dha.gov.ae/Asset%20Library/MarketingAssets/20180611/(E)%20Federal%20Decree%20no.%204%20of%202016.pdf)
- [5] Glenn, C. (2018). HIPPA and protecting health information in the 21<sup>st</sup> century. Retrieved from <https://jamanetwork.com/journals/jama/fullarticle/2682916>
- [6] Goldman, J. (1998). Protecting privacy to improve healthcare. Health affair, Vol. 17, No. 6. Retrieved from <https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.17.6.47>
- [7] Hsu, C.L., Lee, M, R., Su, C. H. (2013). The role of privacy protection in the healthcare information system adoption. Retrieve from <https://link.springer.com/article/10.1007/s10916-013-9966-z>
- [8] John Hopkins. Privacy practices. Retrieved from <https://www.hopkinsmedicine.org/Privacy/>

- [9] Matthan, R. (2018). A new direction for data privacy in healthcare. Retrieved from <https://www.livemint.com/Opinion/3LK0TR6zdXmeIkaJuTUUnnJ/A-new-direction-for-data-privacy-in-healthcare.html>
- [10] Shams, B. (2016). Case Study: Picture of health. *Network Middle East Volume 22, issue 05*. Retrieved from <https://zulekhahospitals.com/uploads/files/NME.pdf>
- [11] The joint commission (2019). Privacy and cookies statement. Retrieved from <https://www.jointcommission.org/en/privacy-and-cookies-statement/>
- [12] Thora, A. J. & Jami, M. V. (2017). Top five privacy and data security issues facing healthcare companies. Retrieved from <https://www.healthcarestat.com/2017/12/top-five-privacy-data-security-issues-facing-healthcare-companies/>
- [13] Thumbay medical tourism. Privacy policy. Retrieved from <http://www.thumbaymedicaltourism.com/privacy>
- [14] World Health Organization- Patient's Rights. Retrieved from <https://www.who.int/genomics/public/patientrights/en/>
- [15] Zuleqa Hospital, privacy policy. Retrieved from <https://www.zulekhahospitals.com/dubai/privacy-policy>