How to Cite:
Muralidharan, M., & Jeyachidra, J. (2022). Patient and healthcare staff viewpoints on EMR access and confidentiality. *International Journal of Health Sciences*, *6*(S8), 6078–6088. https://doi.org/10.53730/ijhs.v6nS8.13712

Patient and healthcare staff viewpoints on EMR access and confidentiality

M. Muralidharan
Research Scholar, Periyar Maniammai Institute of Science and Technology, Vallam, Thanjavur
Email: mi.murali123@yahoo.com

Dr. J. Jeyachidra
Professor, Periyar Maniammai Institute of Science and Technology, Vallam, Thanjavur
Email: chithu_raj@yahoo.co.in

***Abstract*---**A patient's health and well-being, as well as data from at least one healthcare interaction, are included in the EMR system. It may be accessed on a multi-level basis, with authentication according to the user type, inside an institution. The electronic medical record (EMR) system aids doctors in providing better care since it provides a comprehensive medical history for each patient. There are still many misconceptions about electronic medical records (EMR) in the minds of patients and hospital employees throughout the world, and this study aims to fill those gaps. A decade ago, searching PubMed and Google Scholar in addition to several specialized datasets like PsycINFO (Psychiatry Information Services) and Medline (Medical Library) (2007-2017). citations to papers that referenced a certain standard were included in the quality rating process. More than 1,300 entries were considered before just 78 were left for further examination. Access to non-medical information and the opportunity to examine electronic medical data were some of the concerns voiced by patients. However, even the best in-person explanation can't compensate for control over the EMR's content and access. Increased patient knowledge and the capacity to ask questions about the treatment they get and the information shared with others may lead to a dramatic increase in patient lawsuits against healthcare personnel who violate patients' privacy. Better modelling approaches, user training, and frequent refresher sessions all help to improve data security. It boils down to two alternatives for limiting access: using a password or a digital signature.

***Keywords*---**electronic medical record (EMR), electronic health (e-health), medical subject heading (MeSH), health information system (HIS), data protection act (DPA).

Introduction

It's no surprise that Information Technology (IT) is becoming an increasingly important part of the healthcare industry's efforts to improve treatment quality and patient safety. Due to simple internet access and the abundance of medically-related information available online, patients are more concerned and knowledgeable about their symptoms, ailments, and treatment choices [7,9]. When it comes to health information in North America, for example, most people turn to the internet. Decisions on lifestyle changes, medicines and treatment options are also aided by this information. Health records for oneself and other family members are held by 42 percent of Americans, with 87 percent of those retaining paper records [4]. EMR systems have been used in the UAE since 1979, however the Health Authority of Abu Dhabi (HAAD) only completely deployed it in Abu Dhabi in 2008. When it comes to adoption of electronic medical records, Dubai ranked higher than Australia, New Zealand, Malaysia, and Thailand in 2016 based on the EMRAM (Studies in Health Technology & Informatics) (0.06). (0.5).

In terms of patient participation and health outcomes, electronic health (eHealth) technologies are often viewed as having enormous promise. This long-term electronic medical record (EMR) system captures all critical information about a patient's health and well-being from at least one point of contact in a health care establishment [6]. The great majority of hospitals in the United States now employ electronic medical records, or EMRs. Digitalization has made patients more open to this strategy than ever before. A patient's electronic medical record (EMR) may include information about their socioeconomic position, laboratory test results, immunization history, vital signs, current drug regimen, comorbidities, prior medical history, and more (e.g., radiology report, physician report).

Methods

Finding Strategy

Scientists carefully sifted through computer databases to find peer-reviewed scientific publication references relevant to this study (2007-2017). For this research, electronic sources including PubMed, EBSCOhost, and Google Scholar. Medical records, personal health records and patient portals were among the MeSH keywords used to search PubMed, EBSCOhost and Google Scholar for electronic medical records [3]. Numerous items were excluded from this study, such as duplicate articles, coding studies, single-variable datasets (such as prescription or sickness records), letters, editorial, posters and non-English language material.

Results

Patients' Expectations for EMR Content

Interviewees were asked what information they expected to see in their medical records over the course of the interview. There were primarily two schools of thought noticed. To begin with, patients expected general practice records to capture personal data, including socioeconomic situation, in a more thorough manner than hospital records. All respondents agreed that every visit to the doctor would be logged in this manner. It was said that correct diagnosis, safety, and continuity of service were all reasons to preserve such a complete record. According to Malaysia's Penal Code Section 312, if a pregnant woman's life or bodily or mental well-being is in jeopardy, she may only undergo an abortion.

Figure 1: Architecture for Finding Strategy

Due to societal shame and embarrassment, many patients are unwilling to disclose their abortion histories, making it more difficult for the medical community to embrace EMR [2]. Terminations are permissible under certain circumstances, although the law places limits on them. Only a doctor can decide whether or not to carry out a termination in Malaysia, according to the country's Penal Code.

Table 1. Issues which patients are hesitant to disclose in their EMR.

Health Problem	Pertaining to	Notes
Pregnancy	Termination of pregnancy	As a result of the country's strict prohibition on abortion unless in rare circumstances, the topic is considered taboo in Malaysian society. Patients in nations where abortion is legal feel more

		at ease if their healthcare providers are knowledgeable about the issue.
Mental Health	Anxiety/Depression	The care of persons with mental health issues is routinely discriminated against.
Sexual Health concerns	Recommendation for sex treatment / Insufficiency in lust / Need for urgent or routine birth control	The use of contraception, as well as any other concern with a person's sexual health, is considered promiscuous behavior.
Others	Life insurance / Overdose attempt / Medication history	Patients are often afraid of having their insurance coverage cancelled or having their rates soar if they reveal any personal medical information.

The Ability to Access Electronic Medical Records of Individuals

As a relatively recent development in healthcare delivery and information management, patients can now access medical information and clinical treatment through an online portal. Patients may access their own EMR, which includes notes from their physicians and test results, via a variety of websites. They can also send electronic mail to their doctors via these portals. Professionals and patients alike will have access to a whole new realm of possibilities as a result of this development. Many patients can benefit from the availability of a wealth of reliable health data and information in order to better manage their conditions and stay healthy in general [6]. As a relatively new piece of technology, patient online portals let you look for clinical treatment options as well as medical information and resources. Patients may access their own EMR, which includes notes from their physicians, test results, and the ability to send electronic mail to their doctors, through a variety of portals.

Some further benefits include a reduction in medical errors, an increase in the level of care offered, and improvements in patient-related concerns such as appropriateness of treatment. Higher levels of enthusiasm for portal access and use are connected, surprisingly, with dissatisfaction with the doctor-patient connection. Connections such as a lack of communication and a failure to create rapport and difficulties in obtaining crucial medical data are among the reasons for this relationship There are a few issues that limit the broad accessibility to these websites and medical information. Organizational resources (such as computers, internet access, and computer training) and nurses' personal characteristics are just a few of the things that can be improved. Other factors include patients' needs (such as low levels of literacy and e-health literacy, or a lack of social support) and portal-related issues (such as the requirement for more advanced navigational abilities than most patients have Health data and information are readily available to patients, who may utilize this information to better manage their health issues and general well-being. Because EMRs make it possible for doctors and patients to have on-going contact rather than just one-off exchanges, the amount of time spent on problem-solving is also greatly reduced. At any point, it may happen. According to a study conducted in Chicago, Illinois, 95% of the participants (95/106) were satisfied. EMR has a positive effect on patients, according to 59 percent of clinicians who use it (63/107). Some 8/108

participants claimed that their relationship was hindered by the EMR, while 7/108 participants thought that it was good. Keeping in touch with their doctors is essential for them to accomplish this goal. As a consequence, patient desires may be given precedence with such a system.

Access to Patients' Electronic Medical Records by Hcps: A Patient's Point of View

It is important to understand how patients feel about other persons being able to access and use their electronic medical records (EMRs). Rather than a challenge to medical hegemony or an abundance of knowledge for the patient, one study found that vulnerable individuals may not be able to regulate access to data because they lack the capacity. The abuser may have access to the victim's medical records if the victim is a victim of domestic violence, but can the victim avoid this?

Despite this, most individuals are receptive to the concept of their medical data being utilized in research for the "greater good," even if the data is anonymized and identifiable. According to one study, de-identified patient EMRs may be given for research reasons alone, but patients agree that they are confused about how the information will be used, making it difficult to create trust. Almost everyone (98 percent) agrees that the advantages exceed the hazards of exchanging healthcare information with other parties (such as insurance companies). Another poll found that patients want to be able to decide exactly what information is shared with whom, as well as how much information is shared with whom. Patient lists and refill schedules were more commonly shared by patients than direct communication with their doctors.

Patients' Electronic Medical Records Are Available to Hcps

A Health Information System (HIS) implemented in several Malaysian hospitals has improved access to medical records and increased efficiency in healthcare delivery. Physical storage, search and retrieval of medical records are now unnecessary because all workstations have computers that can access the patient's data. Patients' records are less likely to be lost if they are kept in an electronic database. HCPs can respond quickly and provide care to patients because of the advantages of easy access to patient information. When a patient is unable to offer essential information because of a major injury or illness, this is extremely important.

The electronic medical record (EMR) must be controlled in order to preserve patients' privacy and to maintain patient-provider confidence. Audit trails and access control are implemented to ensure that medical records are kept private. Users' names, dates and locations are recorded in audit trails when they access data. It aims to discover security breaches, duplicate security incidents, and prevent future occurrences of the same. The Malaysian Ministry of Health established a policy and guidelines for EMR in December 2011 to protect patient privacy and regulate the creation, storage, and utilization of clinical information systems.

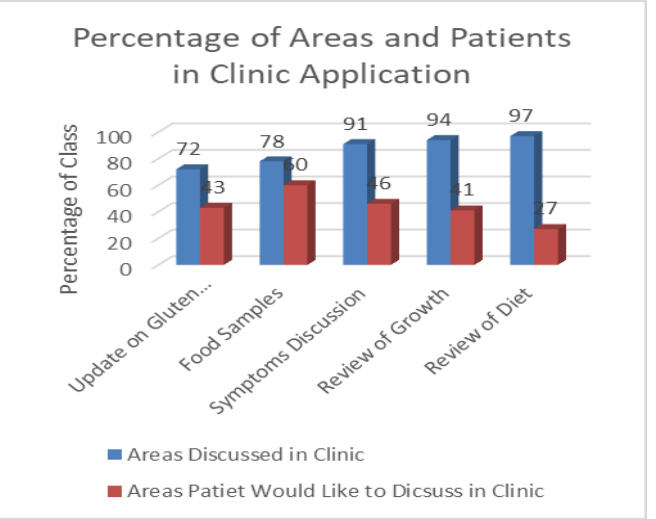

Figure 2: Percentage of Areas and Patients in Clinic Application

It provides as a blueprint for the implementation of operational access control rules and processes in all Malaysian healthcare institutions. There must be clear criteria for who gets access to patient information and the limitations on how that information may be used because interdisciplinary teams are widespread in healthcare settings. In addition to direct patient treatment, patient data is utilized for a variety of additional purposes. As a result, users are either categorized as major or secondary based on their level of importance. The primary users are those who utilize patient information to manage a patient's health. Users of patient data in the secondary category include people who utilize it for activities such as quality control audits, research, and education. The usage of medical records for secondary purposes is also governed by a user access control policy.
The following are the norms and regulations governing the secondary use of patient information:

I. There will be restrictions and cautions on the use of data extraction tools.
II. Only with the patient's permission may a third-party access patient data.
III. If the patient agrees to seek care from another practitioner, discharge reports will be provided.
IV. Patient records will be de-identified in order to conduct audits and ensure the quality of the care provided.

Ethical review boards in medical facilities will determine the quantity of data that can be used for research purposes. To educate patients, patients must provide their consent.

The electronic medical record (EMR) must be controlled in order to preserve patients' privacy and to maintain patient-provider confidence. Systems such as audit trails and access restrictions are in place to preserve patient information's privacy. Users' names, dates and locations are recorded in audit trails when they access data. It aims to discover security breaches, duplicate security incidents, and prevent future occurrences of the same. The Malaysian Ministry of Health

established a policy and guidelines for EMR in December 2011 to protect patient privacy and regulate the creation, storage, and utilization of clinical information systems. It provides as a blueprint for the implementation of operational access control rules and processes in all Malaysian healthcare institutions.

User roles and access to medical records are established in a standard operating environment using a user control matrix. Patient care doctors can see demographic information and clinical data but not the financial invoices of the patients they treat at the hospital, for example. While on-call or after a patient has been referred to their department, certain jobs can bypass access limitations. Instead of automatically notifying the facility director, they will be prompted to provide a justification for requesting the access override.

Perspectives of Hcps on Patient Access to Electronic Medical Records

Studies have found that doctors are divided on the subject of patients being able to see their medical information. Dr. Opinions on patient access vary but doctors are generally in favor of patients having access to their medical records.' To begin, doctors noted that allowing patients access to their medical information increases transparency, which strengthens the doctor-patient relationship, creates mutual trust, and facilitates discourse during appointments. Reports indicated that people were feeling more empowered and happier with their care. It's been reported that the way doctors record sensitive information, such as drug usage or mental health difficulties, has changed as well.

This is done in order to keep patients from experiencing bad feelings as a result of using language that is too direct. When people are educated about their own health and issues, they are more likely to take control of their own health care. Study after study has found that patients who had access to their doctor's notes were more likely to stick with their medical regimens because the notes serve as a reminder. Unlike patients, doctors are concerned about causing needless tension and worry by being open and honest. The ramifications of making a mistake in a doctor's notes, especially on a busy day, are unusual for professionals to be concerned about. Giving patients access to their medical information has both advantages and risks. When it comes to their own health, patients have a professional and ethical duty to act in their own best interests, and to decide how much and what information they give.

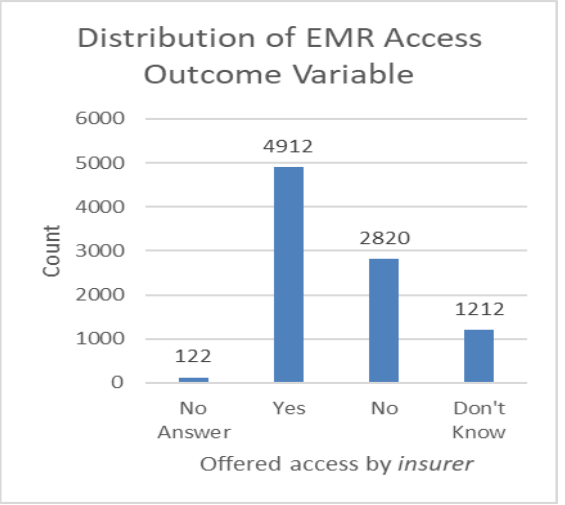

Figure 3: Distribution of EMR Access Outcome Variable

Concerns Regarding EMR Confidentiality

Medical secrecy serves two key reasons. An important first step is to ensure that patients don't feel vulnerable or embarrassed because of their treatment. Second, the doctor-patient connection sets the stage for open dialogue. Maintaining secrecy in today's modern health care system, which is delivered by a variety of teams, is notoriously difficult. From different national policies to different views within the profession, there appears to be a struggle.

Patients' freedom, social benefit, and "innocent other" protection may all play a role in a patient's lack of trust in the medical system. But on the other hand, there are strong justifications for complete confidentiality. Combined with the Human Rights Act of 1998, a shift in control over personal data was brought about by the Data Protection Act (DPA). All personal data is now owned by the data subject (patient) in its full, and no one else may access it. The Data Protection Act of 1998 is summarized in Table 3. Medical confidentiality is not a universal duty under common law. Legislative circumstances that necessitate the disclosure of secret information justify a breach of confidentiality. If a patient's competence to give informed consent has been established. Confidentiality can be waived if the consequences of a disclosure are sufficiently dire.

Discussion

There were 37 percent and 36 percent of respondents to a poll on broad beliefs on privilege who agreed with the notion but felt that it should not be absolute, respectively. There should be a right to reveal information in some cases, stated 88% of the respondents, and 41% agreed. The participants were well-protected.

Table 2. Legal and ethical issues in telemedicine

Fundamental aspects of telemedicine Fundamentals of ethics - a patient-professional relationship that is characterized by confidentiality, autonomy and consent, beneficence and nonmaleficence, fairness and accessibility
Problems primarily impacting the use of telemedicine Using and Disseminating Health Data - Consent to information sharing, confidentiality, privacy and data protection, and management of information security Accountability, culpability, and best practices - indemnity insurance, clinical governance, registration and training, Duty of care, and risk management are all aspects of clinical governance and risk management. Best practices, standards, and guidelines - The origin, evolution, and substance of previously published guidelines, standards, and protocols
Issues primarily impacting telemedicine supply Providing telemedicine services - E-commerce and distance selling legislation; advertising of medical and pharmaceutical items; rules governing the use of media and broadcasting Interoperability and standards - 'standards bodies, A Different Approach' Directives, and public-sector procurement duties Medical equipment, product responsibility, and safety are all issues that need to be addressed. - Medical device legislation, CE marking, FDA approval, Product Liability Directives, and General Product Safety Rights to intellectual property - trademarks, Copyright, patents, design rights, passing off and other infringements, and exploitation are all examples of infringements.

Furthermore, a survey of 5330 West London residents revealed that having their medical records stored in one central location would make them more content. Anxiety and skepticism about the EMR system's security were expressed by 79 percent of respondents. As a matter of principle, secrecy is a matter of degree. EMR confidentiality is not addressed under any existing ethical or legal norms. There are occasions when a breach of trust must be disclosed in order to prevent harm to the patient or society at large, especially in the doctor-patient relationship. As long as the patient's integrity is respected and protected, everything else will fall into place. Today, it's critical to debunk the myth that transferring data over an EMR system renders it more susceptible to attack. In order for the EMR to work as a safe haven for personal data, patients must be informed on how it prioritizes confidentiality and provides only the information that is absolutely essential for their treatment.

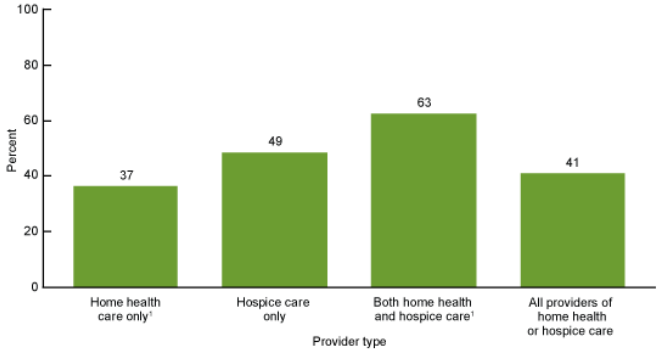

Figure 3: Distribution of Healthcare across various Scenario

Combined with the Human Rights Act of 1998, a shift in control over personal data was brought about by the Data Protection Act (DPA). All personal data is now owned by the data subject (patient) in its full, and no one else may access it. As a reminder, here are some key points from the Data Protection Act of 1998:

Conclusion

EMR confidentiality is a hot-button issue for patients, and this study indicated that patients' expectations about confidentiality are not always met in practice. One in five people didn't even know their personal EMR was accessible to healthcare professionals other than doctors. There were also concerns about doctors' access, with most respondents believing that no administrative, financial, or other staff members should have access. It was also mentioned throughout the meeting that non-medical data should be recorded in the EMR. Patients' de-identified electronic medical records (EMRs) were seen as a safe haven from those with access, ensuring that the data would not be misused or mismanaged. Doctor-to-patient interactions were seen as a positive development by patients since a good explanation in person is still preferable to total control of content and access to electronic medical records (EMR).

Physicians and the EMR team must work collaboratively to ensure that all patients' privacy is maintained. Medical malpractice lawsuits are projected to grow in the future as individuals become more aware and empowered to raise concerns about the treatment, they are receiving from their healthcare providers. These problems need that patient groups be better informed and have access to the necessary equipment. To increase information security, improved risk and vulnerability modelling methodologies may be used. End-user training and refresher courses should need a password or digital signature to access.

References

1. “A Blockchain-Based Credibility Scoring Framework for Electronic Medical Records” S Siva Rama Krishnan;M.K Manoj;Thippa Reddy Gadekallu;Neeraj Kumar;Praveen Kumar Reddy Maddikunta;S. Bhattacharya;D. Y. Suh;M. J. Piran 2020 IEEE Globecom Workshops (GC Wkshps_2020.
2. “A Reference Architecture Approach for Pathway-Based Patient Integration” Martin Benedict;Hannes Schlieter;Martin Burwitz;Tim Scheplitz;Marcel

Susky;Peggy Richter 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC)_2019.

3. “A study for evaluating the suitability of peritoneal dialysis(PD) patients with occupational attribute questionnaire” Wang-Chin Tsai;Shuo-He Wang 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)_2019.
4. “Designing Health Interface Technologies to Support Patients’ and Healthcare Providers’ Individual and Collaborative Work” Tera L. Reynolds 2020 IEEE International Conference on Healthcare Informatics (ICHI)_2020.
5. “Effect of Patient Online Information Searching on the Trust in the Doctor——A Cognitive Dissonance Theory Perspective” Yongmei Liu;Xiangxi Lei 2019 Chinese Control And Decision Conference (CCDC)_2019.
6. “On the Design of a Blockchain-as-a-Service-Based Health Information Exchange (BaaS-HIE) System for Patient Monitoring” Alina Buzachis;Antonio Celesti;Maria Fazio;Massimo Villari 2019 IEEE Symposium on Computers and Communications (ISCC)_2019.
7. “Privacy Preservation for Outsourced Medical Data With Flexible Access Control” Xingguang Zhou;Jianwei Liu;Qianhong Wu;Zongyang Zhang IEEE Access_2018.
8. “Privacy-Preserving Traceable Attribute-Based Keyword Search in Multi-Authority Medical Cloud” Qinlong Huang;Guanyu Yan;Yixian Yang IEEE Transactions on Cloud Computing_2021.
9. “Secure and Privacy-aware Blockchain-based Remote Patient Monitoring System for Internet of Healthcare Things” Bessem Zaabar;Omar Cheikhrouhou;Meryem Ammi;Ali Ismail Awad;Mohamed Abid 2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)_2021.
10. “Secure Storage of Electronic Medical Records(EMR) on Interplanetary File System(IPFS) Using Cloud Storage and Blockchain Ecosystem” Swadhin Routray;Raghavendra Ganiga 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT)_2021.
11. “Software Engineering with Conflicting User Needs: Patient Accessible Electronic Patient Records” Åsa Cajander 2018 IEEE/ACM International Workshop on Software Engineering in Healthcare Systems (SEHS)_2018.
12. “Vision-based Bed Detection for Hospital Patient Monitoring System” Madoka Inoue;Ryo Taguchi;Taizo Umezaki 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)_2018.