International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cognizance About Privacy and Security of Patients Health Information Among Medical and Dental Students

Dr. A. Vinita Mary[1], Dr. R. Kesavan[2], Dr. Vaishnavi.V[3], Allwyn Susil.A[4], Akshaya Tharini.P[5], Aysha Sherine Rahuman[6]

[1]MDS, PhD, Professor and Head, Department of Public Health Dentistry, Thai Moogambigai Dental College and Hospital, Chennai, Tamil Nadu, India
[2]MDS, Department of public health dentistry, Thai Moogambigai Dental College and Hospital, Chennai, Tamil Nadu, India
[3]BDS, Lecturer,Department of public health dentistry, Thai Moogambigai Dental College and Hospital, Chennai, Tamil Nadu, India
[4,5,6]Student, Thai Moogambigai Dental College and Hospital, Chennai, tamil Nadu, India

Abstract:

Background: The proliferation of electronic health records and digital medical systems has brought about significant advancements in patient care and information management. However, concerns regarding the privacy and security of patients' health information have also intensified. As future healthcare practitioners, medical and dental students play a pivotal role in ensuring the safeguarding of sensitive patient data. This study aims to assess the awareness and understanding of privacy and security issues related to patients' health information among medical and dental students.

Methods: A cross-sectional study was conducted among a representative sample of medical and dental students from diverse academic institutions. A structured questionnaire was administered to assess participants' knowledge, attitudes, and practices concerning patient data privacy and security. Descriptive statistics were used to analyse the data, and associations between demographic factors and awareness levels were explored.

Results: The study findings reveal that while a substantial portion of medical and dental students recognize the importance of patient data privacy, a significant knowledge gap exists regarding the specific measures and protocols to ensure security. The research found that 232(71.7%) of the participants preferred electronic patient records for their ease of accessibility and 198 (61.4%) strongly valued privacy. Students expressed varying levels of understanding concerning encryption methods, access controls, and legal frameworks governing patient information.

Conclusion: This study underscores the imperative for comprehensive education and training programs focusing on privacy and security of patients' health information within medical and dental curricula. As future healthcare practitioners, medical and dental students must be equipped with the necessary skills and knowledge contributing to a more secure and privacy-aware healthcare environment.

Keywords: Healthcare, Data Protection laws, electronic records.

INTRODUCTION

In the rapidly evolving landscape of healthcare, the digitization of patient health information has brought forth unprecedented opportunities for improved patient care, research, and data management. The electronic exchange of health records and the utilization of digital health platforms have become integral components of modern healthcare systems.[1] However, this digital transformation has also ushered in new challenges, particularly concerning the privacy and security of patients' health information.

The national adoption of electronic health records (EHR) promises to make an unprecedented amount of data available for clinical research, ensuring the confidentiality and protection of this sensitive data is not only a legal and ethical imperative but also a crucial factor in maintaining patient trust and upholding the integrity of the healthcare system.[2] The proliferation of health emergencies, such as epidemics, natural disasters, and artificial crises, further underscores the urgency of this investigation. In times of crisis, the availability, accuracy, and security of health information become paramount for effective decision-making and response coordination.[3]

The global pandemic COVID-19 has vividly demonstrated the critical role of electronic health records (EHRs) and digital health data exchange in managing public health emergencies. As the pandemic highlighted the interconnectedness of healthcare systems and the need for swift and secure information sharing, it has also accentuated the significance of equipping future healthcare practitioners with the knowledge and skills to ensure the privacy and security of patient health information.[4] In this context, medical and dental students represent the future of healthcare, poised to play a pivotal role in shaping and navigating the complexities of the digital healthcare landscape. As these students prepare to become healthcare practitioners, it is imperative that they possess a comprehensive understanding of the privacy and security considerations associated with handling patient health information. Their awareness and adherence to best practices in data protection will significantly influence the effectiveness and integrity of healthcare delivery, research, and patient trust. This study seeks to contribute to the broader discourse on healthcare data management and privacy by shedding light on the current state of awareness among medical and dental students.

MATERIALS AND METHODS

A structured questionnaire was designed which collected information on the demographics of the study population and comprised 14 questions that addressed awareness of data privacy and security concepts, familiarity with encryption methods and access controls, and perceptions about the importance of patient health information protection. The study was approved by the ethics committee board of Dr. MGR Educational and Research Institute, Chennai, India. The questionnaire was circulated amongst medical and dental students across various states in India as google forms via social media platforms-WhatsApp, Gmail, Instagram over a period of 4 months and the total responses, i.e., 323 responses, were included in this study. To analyse the data SPSS IBM SPSS Statistics for Windows, Version 23.0, Armonk, NY: IBM Corp. Released 2015 was used to calculate frequency and percentage of the variables. The level of significance was fixed as 5% ($\alpha = 0.05$)

RESULTS

In a study conducted with 323 participants, the respondents were primarily from Tamil Nadu, the age range of the sample ranged from 17 to 29 with mean age being 20.23$\pm$1.79, with a majority of 237 participants being females (73.3%). Notably, a significant portion, 211 (65.3%), were pursuing dental

education, and 244 (75.5%) were attending private colleges. The research found that 232 (71.7%) of the participants preferred electronic patient records for their ease of accessibility, and 198 (61.4%) strongly valued privacy. Security measures varied, with 127 (39.3%) indicating that staff education was part of these measures, and a substantial 246 (76.0%) used CCTV for security. Most institutions, 263 (81.4%), informed patients about data usage, but only 98 (30.3%) retained records for 10 years. Additionally, 191 (59.2%) of the participants reported mechanisms for data deletion, and 138 (42.7%) mentioned the use of biometric systems. Interestingly, 212 (65.6%) of the respondents were aware of an Indian patient data security act. These findings shed light on the preferences and security measures that were in place within the context of patient data management.

Table 1- Demographic Details of the study participants

	Options	**Frequency**	**Percent**
Gender	**Male**	87	26.9
	Female	237	73.1
Course	**Medical**	74	22.8
	Dental	211	65.1
Type of college	**Government college and hospital**	47	14.5
	Private college affiliated to deemed university	244	75.3
	Private college affiliated to government university	33	10.2
Year of study	**1st year**	163	50.3
	2nd year	18	5.6
	3rd year	56	17.3
	4th year	31	9.6
	CRRI	52	16.0
	Post graduate	4	1.2
State	**Andhra Pradesh**	4	1.2
	Goa	1	0.3
	Himachal Pradesh	1	0.3
	Jammu and Kashmir	1	0.3
	Kerala	9	2.8
	Rajasthan	1	0.3
	Tamil Nadu	304	93.8
	Telangana	1	0.3
	Uttar Pradesh	1	0.3
	West Bengal	1	0.3

Table 2- Knowledge, attitudes, and practices concerning patient data privacy and security among the study participants

	Options	Frequency	Percent
Which type of patient records does your institution maintains?	**Paper based**	211	65.1
	Software based	85	26.2
	Online based	28	8.6
Which is your favourite method of preference for patient record management?	**Paper based records**	92	28.4
	Electronic based records	232	71.6
Why do you prefer the chosen method of patient record management?	**Easy handling**	115	16.88
	Easy accessibility and retrievability	174	25.55
	Easy to use	141	20.70
	Patient can view their records	111	16.29
	Backup records easily	140	20.55
Do you think maintaining privacy of patient data is important in health care?	**Strongly agree**	198	61.1
	Agree	85	26.2
	Neutral	29	9.0
	Disagree	8	2.5
	Strongly disagree	4	1.2
How does your institution maintain the privacy of patient's healthcare data?	**Security risk assessment**	85	17.59
	Encrypt all patient data	123	25.46
	Electronic health record (EHR) software and hardware	112	23.18
	Staff education and training	127	26.29
	EHR access controls	34	7.03
	None of the above	2	0.414
What do you think about importance of integrating	**Personal autonomy**	41	12.7
	Dignity and worth as human beings	33	10.2

privacy and security about patient information?	**Maintain relationship with patient**	21	6.5
	All the above	229	70.7
Why do you think we need privacy and security in patient data management?	**To promote and maintain fundamental medical ethical principle**	38	11.7
	To meet social expectations	25	7.7
	To Building trust between patients and medical professionals	25	7.7
	To Maintain confidentiality	17	5.2
	All the above	219	67.6
Do your institution have any ways to monitor security incidents continuously?	**Threat detection**	51	10.51
	Malware attack	40	8.24
	Intrusion Detection and Prevention Systems	60	12.37
	CCTV	246	50.72
	Locker rooms	88	18.14
What do you think can view the patient's health record?	**Doctors**	80	24.7
	Nurses	12	3.7
	Insurance	11	3.4
	Patient	12	3.7
	All the above	209	64.5
Do you inform your patients about how you use or disclose their health information?	**Yes**	262	80.9
	No	62	19.1
How long should patient's health records be maintained?	**3 years**	91	28.1
	5 years	90	27.8
	7 years	45	13.9
	10 years	98	30.2
Does your institution have any mechanism to	**Yes**	191	59.0
	No	133	41.0

destroy or delete health information records id requested to do so			
Is there any security solutions to manage patients health record privacy in your institution?	**Private examination and consultation rooms**	165	38.55
	Attention to eavesdropping risk	58	13.55
	Passwords, biometric identification	138	32.24
	Automatic logouts	67	15.33
Are you aware of any patient data security act present in India?	**Yes**	212	65.4
	No	112	34.6

DISCUSSION

A cross-sectional study was conducted to assess the cognizance about privacy and security of patients' health information among medical and dental students. Out of a total 323 participants in the study, a substantial portion 198(61.1%) comprising medical and dental students strongly agreed that maintaining the privacy of patient data was crucial. Pratiwi AB et al.'s study in Indonesia revealed that general practitioners and dentists at primary health care centers also shared similar views in expressing a need to uphold patient privacy.[11]

The participants in the present study cited reasons for choosing electronic records over conventional paper-based records, such as easy handling, accessibility, retrievability, user-friendliness, patient access, and efficient backup options. This preference reflects a shift towards embracing technology for enhanced efficiency and accessibility in managing patient records.

The present study revealed participants employing various methods, including security risk assessment, encryption, EHR software and hardware, staff education, and access controls in their respective institutions to ensure data security. This emphasis aligns with the results of Masresha Derese Tegegne's study, where majority of participants also highlighted the significance of these factors.[7]

Data security is a fundamental element of comprehensive privacy practices, as emphasized by Hodge et al.[12] About 229(70.7%) respondents overwhelmingly agree on the importance of integrating privacy and security for reasons such as personal autonomy, human dignity, maintaining relationships with patients, and adherence to medical ethical principles. The primary reasons for ensuring privacy and security in patient data management included upholding ethical principles, meeting societal expectations, building trust between patients and medical professionals, and maintaining confidentiality.

The present study acknowledges the ongoing challenges related to maintaining data privacy and security in the healthcare sector, which resonate with the findings of Redspin's 7th annual breach report on Protected Health Information (PHI). These findings underscore the potential adverse effects of security breaches, including economic harm, social and psychological harm, and identity theft, as corroborated by the study

conducted by Gostin et al.[10]. The data from our questionnaire indicates that healthcare institutions employ various methods, including threat detection, malware attack monitoring, intrusion detection and prevention systems, CCTV, and locker room security, to continuously monitor security incidents. This proactive approach suggests a commitment to identifying and addressing potential security threats promptly. While these systems offer advanced healthcare services, there is a growing awareness of security issues concerning e-health data, which contains highly sensitive information.[13]

In the present study, most respondents 209(64.5%) believed that doctors, nurses, insurance, and patients should have access to patient health records. Also, a majority of 262 (80.9%) of them agreed that they inform their patients regarding how their health information is used or disclosed and this demonstrates transparency and compliance with privacy regulations. There exists a varying opinion regarding the duration of maintaining patient health records. While a significant portion suggested 10 years 98(30.2%), others favoured shorter durations like 3 years 91(28.1%) and 5 years 90(27.8%).

A notable majority 191(59.0%) confirmed having mechanisms instilled by their institutions to destroy or delete health information records upon request. Eliminating health records upon request is good as it respects patient privacy, complies with data protection laws, enhances security, and fosters trust in patients through transparency. It also aligns with ethical principles, accommodates changing patient preferences, and helps limit unnecessary data retention.

The respondents in our study confirmed that there were various security solutions, including private examination and consultation rooms, eavesdropping risk attention, passwords, biometric identification, and automatic logouts, all of which were employed to avoid breaching of privacy regarding patient health information by their institutions. A substantial majority 212(65.4%) were aware of the patient data security act in India, indicating a greater consciousness of regulatory frameworks governing patient data.

CONCLUSION

The study revealed that medical and dental students generally have a high level of awareness regarding the privacy and security of patients' health information. This awareness is a positive sign as it reflects the recognition of the sensitive nature of patient data in healthcare settings and there is growing recognition of importance of digital solutions, privacy, and security in managing patient records in the healthcare sector in India. These findings also suggest that educational institutions play a significant role in fostering awareness among students and highlights the importance of incorporating data privacy and security into the curriculum.

REFERENCES

1. Harahap NC, Handayani PW, Hidayanto AN. Functionalities and Issues in the Implementation of Personal Health Records: Systematic Review. J Med Internet Res. 2021 Jul 21;23(7):e26236. doi: 10.2196/26236. PMID: 34287210; PMCID: PMC8339989.
2. George Hripcsak , David J Albers, Next-generation phenotyping of electronic health records, *Journal of the American Medical Informatics Association*, Volume 20, Issue 1, January 2013, Pages 117–121,
3. Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *J Am Med Inform Assoc.* 2006;13(2):121–126. doi: 10.1197/jamia.M2025.
4. Bouri N, Ravi S. Going mobile: how mobile personal health records can improve health care during emergencies. *JMIR Mhealth Uhealth.* 2014;2(1):e8. doi: 10.2196/mhealth.3017.

5. Abouelmehdi, K., Beni-Hessane, A. & Khaloufi, H. Big healthcare data: preserving security and privacy. *J Big Data* **5**, 1 (2018).
6. Zanaboni P, Kummervold PE, Sørensen T, Johansen MA. Patient Use and Experience With Online Access to Electronic Health Records in Norway: Results From an Online Survey. J Med Internet Res. 2020 Feb 7;22(2):e16144. doi: 10.2196/16144. PMID: 32031538; PMCID: PMC7055829.
7. Tegegne MD, Melaku MS, Shimie AW, Hunegnaw DD, Legese MG, Ejigu TA, Mengestie ND, Zemene W, Zeleke T, Chanie AF. Health professionals' knowledge and attitude towards patient confidentiality and associated factors in a resource-limited setting: a cross-sectional study. BMC Med Ethics. 2022 Mar 14;23(1):26. doi: 10.1186/s12910-022-00765-0. PMID: 35287659; PMCID: PMC8922732.
8. Couper MP, Singer E, Conrad FG, Groves RM. Risk of Disclosure, Perceptions of Risk, and Concerns about Privacy and Confidentiality as Factors in Survey Participation. J Off Stat. 2008;24(2):255-275. PMID: 21603156; PMCID: PMC3096944.
9. UNC Health Care relies on analytics to better manage medical data and improve patient care. IBM Press release. 2013.
10. Gostin L. Public health law: Power, duty, restraint. Berkeley, CA: University of California Press; 2008. Surveillance and public health research: Personal privacy and the "right to know."
11. Pratiwi AB, Padmawati RS, Willems DL. Behind open doors: Patient privacy and the impact of design in primary health care, a qualitative study in Indonesia. Front Med (Lausanne). 2022 Oct 19;9:915237. doi: 10.3389/fmed.2022.915237. PMID: 36341251; PMCID: PMC9626974.
12. Hodge JG Jr, Gostin LO, Jacobson PD. Legal issues concerning electronic health information: Privacy, quality, and liability. JAMA. 1999;282(15):1466–1471.
13. Oh SR, Seo YD, Lee E, Kim YG. A Comprehensive Survey on Security and Privacy for Electronic Health Data. Int J Environ Res Public Health. 2021 Sep 14;18(18):9668. doi: 10.3390/ijerph18189668. PMID: 34574593; PMCID: PMC8465695.