Introduction structure for this paper.  
- Benefits of EHR over paper-based health record system

- Challenges of EHR (Especially security and privacy since  
health data can be accessed over the Internet)  
- Role of law, policies, and regulations to overcome EHR  
challenges and protect healthcare data security and patient  
privacy  
- Consequences of policy violations (HHS OCR com-  
plaints, some security and privacy incidents, data breach,  
health insurance fraud)  
- Fundamental reasons for policy violations (not rigorous  
enforcement mechanism, professional subcultures, differ-  
ent set of policy bodies, improper or lack of required  
training for health workers)

Introduction

Electronic Health Records (EHRs) improve healthcare by providing immediate and remote access to patient information, reducing errors associated with paper records, and streamlining workflows for enhanced efficiency over paper-based health record system [1,3]. They promote interoperability, allowing seamless data sharing among different healthcare providers, ultimately contributing to better continuity of care.EHRs also offer cost savings through the elimination of paper-related expenses and improved resource allocation [2].

Data privacy and security issues is the foremost concerns of EHR.Cybersecurity risks, potential breaches, and the need for stringent access controls raise significant questions.Additionally, interoperability issues, human factors such as user authentication, and the imperative of legal compliance further compound the challenges associated with the implementation and maintenance of EHR systems [5,6]. According to the Information Security Media Group, 75% of surveyed healthcare organizations in the US reported at least one security breach affecting less than 500 individuals, and 21% reported an incident affecting more than 500 individuals. The Healthcare Information and Management Systems Society found that 68% of surveyed healthcare organizations in the US experienced a significant security incident. These incidents were reported to be caused by both insider threats (53.7%) and external threats (63.6% of healthcare organizations). It is important to note that these reported incidents may not capture all security breaches, as some incidents go undetected or are underreported. The security breaches in healthcare can be costly, with cases of breaches in healthcare data costing hospitals between US 250000 to US 2.5 million in settlement payments.[4]

Law, policies, and regulations play a pivotal role in addressing EHR challenges and safeguarding healthcare data security and patient privacy.In various global regions, diverse privacy standards, including the General Data Protection Regulation (GDPR) in Europe, the Health Insurance Portability and Accountability Act (HIPAA) in the United States (US), and My Health Record (MHR) in Australia have been established to protect patient privacy and personal data [8] . The HIPAA policy standards and guidelines that help mitigate the risks associated with EHR and promotes trust between patients and healthcare providers.HIPAA requires healthcare organizations to implement technical, administrative, and physical safeguards to secure EHRs [7]. These safeguards include access controls, encryption, authentication measures, and regular security assessments. By enforcing these safeguards, HIPAA helps prevent unauthorized access, data breaches, and identity theft.Furthermore, HIPAA mandates the implementation of privacy policies and procedures to govern the use and disclosure of patient information. It grants patients certain rights, such as the right to access and amend their medical records and requires healthcare providers to obtain patient consent for certain uses and disclosures of their information.

HIPAA also establishes penalties for non-compliance, which incentivizes healthcare organizations to prioritize data security and privacy. These penalties can range from fines to criminal charges, depending on the severity of the violation. The violation can also lead to reputational damage, eroding trust from clients and the public. Organizations may face exclusion from federal programs, financial strain due to legal costs, and increased scrutiny. The violation of HIPPA can also leads to provider confusion, increased documentation time, alert fatigue, and potential patient safety issues[9]. The Office of Civil Rights Data study showed that over half of the population in the USA might have been affected by security breaches since October 2009 [10]. At least 173 million medical records breached due to the policy non compliance. The study showed that the hackers recruited the health care insiders with access to valuable data `using online ads and social media.

The significant rise in data breaches is heavily influenced by the existence of distinct professional subcultures within the healthcare sector [11]. The healthcare professionals may have their own norms and practices. Misalignment between these subcultures and established policies can lead to non-compliance. Another important factor which contributes to policy violation is insufficient enforcement mechanism due to different set of policy bodies. Healthcare is often subject to a complex web of regulations and guidelines established by different organizations, both at the national and international levels. This multiplicity of policy bodies can create challenges and potential conflicts for healthcare providers and professionals [12, 13]. Analysis of data from the United States Department of Health and Human Services, covering data breaches recorded from January 2015 to December 2020, revealed that a significant portion of the compromised data resulted from insufficient communication and training for healthcare professionals. Inadequate communication and training contribute to policy violations in healthcare by leaving staff unaware of existing policies or changes, leading to unintentional non-compliance. Insufficient training exacerbates challenges in understanding complex policies, increasing the risk of improper implementation. Additionally, communication gaps between departments, limited feedback mechanisms, and cultural barriers further hinder effective policy adherence among healthcare professionals [14].

Top of Form

[1] Silow-Carroll, Sharon, Jennifer N. Edwards, and Diana Rodin. "Using electronic health records to improve quality and efficiency: the experiences of leading hospitals." Issue Brief (Commonw Fund) 17.1 (2012): 40.

[2] Highfill, Tina. (2019). Do hospitals with electronic health records have lower costs? A systematic review and meta-analysis. International Journal of Healthcare Management. 13. 1-7. 10.1080/20479700.2019.1616895.

[3] Jindal, S.K. and Raziuddin, F. (2018), "Electronic medical record use and perceived medical error reduction", International Journal of Quality and Service Sciences, Vol. 10 No. 1, pp. 84-95. <https://doi.org/10.1108/IJQSS-12-2016-0081>.

[4] Keshta, Ismail, and Ammar Odeh. "Security and privacy of electronic health records: Concerns and challenges." *Egyptian Informatics Journal* 22.2 (2021): 177-183.

[5] Mathai, N., M. F. Shiratudin, and F. Sohel. "Electronic health record management: expectations, issues, and challenges." *Journal of Health & Medical Informatics* 8.3 (2017): 1-5.

[6] Bayer, Ronald, John Santelli, and Robert Klitzman. "New challenges for electronic health records: confidentiality and access to sensitive health information about parents and adolescents." *Jama* 313.1 (2015): 29-30.

[7] Mbonihankuye, Scholas, Athanase Nkunzimana, and Ange Ndagijimana. "Healthcare data security technology: HIPAA compliance." Wireless communications and mobile computing 2019 (2019): 1-7.

[8]S. M. Shah and R. A. Khan, "Secondary Use of Electronic Health Record: Opportunities and Challenges," in IEEE Access, vol. 8, pp. 136947-136965, 2020, doi: 10.1109/ACCESS.2020.3011099.

[9] Berg, Gina M., Taylor Shupsky, and Kevin Morales. "Resident Indentified violations of usability heuristic principles in local electronic health records." *Kansas Journal of Medicine* 13 (2020): 84.

[10] Koczkodaj, Waldemar W., et al. "Massive health record breaches evidenced by the office for civil rights data." *Iranian Journal of Public Health* 48.2 (2019): 278.

[11] Sarkar, Sumantra, et al. "The influence of professional subculture on information security policy violations: A field study in a healthcare context." *Information Systems Research* 31.4 (2020): 1240-1259.

[12] Garpenby, Peter, and Ann-Charlotte Nedlund. "The patient as a policy problem: Ambiguous perceptions of a critical interface in healthcare." *Health* 26.6 (2022): 681-701.

[13] Fowler, Luke. "How to implement policy: Coping with ambiguity and uncertainty." *Public Administration* 99.3 (2021): 581-597.

[14] Yeo, Liu Hua, and James Banfield. "Human factors in electronic health records cybersecurity breach: an exploratory analysis." *Perspectives in Health Information Management* 19.Spring (2022).