EPH - International Journal Of Medical And Health Science
ISSN (Online): 2456-6063
Volume 08 Issue 02 June 2022
DOI: https://doi.org/10.53555/eijmhs.v8i2.183

CONFIDENTIALITY IN HEALTHCARE: A COMPARATIVE ANALYSIS OF PAPER-BASED AND ELECTRONIC HEALTH RECORD SYSTEMS

AL Mutairi, Osamah Mousa[1*], AL Harbi, Rashed Faisal[2], AL Harbi, Ahmed Badae[3], AL Harbi, Mohammed Shabeeb[4], AL Harbi, Talal Muteb[5], AL Mohesen, Sultan Abdullah[6], AL Harbi, Mohammed Badday[7]

[1]Ministry of National Guard Health Affairs, almutairios@mngha.med.sa*
[2]Ministry of National Guard Health Affairs, alharbira10@mngha.med.sa
[3]Ministry of National Guard Health Affairs, alharbiah10@mngha.med.sa
[4]Ministry of National Guard Health Affairs, alharbim26@mngha.med.sa
[5]Ministry of National Guard Health Affairs, alharbita7@mngha.med.sa
[6]Ministry of National Guard Health Affairs, almohesensu@mngha.med.sa
[7]Ministry of National Guard Health Affairs, alharbim28@mngha.med.sa

Corresponding Author:
almutairios@mngha.med.sa

Abstract:

The transition from paper-based to Electronic Health Record (EHR) systems is transforming healthcare management. Although EHRs offer operational advantages like efficiency, ease of access, and cost-saving, they present new challenges in maintaining the confidentiality of sensitive patient information. This article provides a comprehensive comparison between paper-based and EHR systems in terms of confidentiality measures, examining aspects such as physical security, access control, data sharing and transfer, and legal frameworks. Traditional paper records, stored in secure physical locations and accessed only by authorized personnel, have limitations like inefficiency and difficulty in data sharing. Conversely, EHRs, while efficient and easily accessible, are susceptible to risks like hacking and unauthorized access. Both systems fall under healthcare confidentiality laws like HIPAA in the United States or GDPR in Europe, but EHRs introduce complexities that are still under legal scrutiny. Understanding the unique risks and benefits of each system is crucial for healthcare providers to make informed decisions that protect patient confidentiality in this digital age.

Keywords: *Confidentiality, Healthcare, Paper-Based Systems, Electronic Health Records (HER), Security, Data Sharing, Auditing, HIPAA, GDPR.*

1. INTRODUCTION:

The healthcare landscape has undergone significant transformation over the years, moving from traditional paper-based health records to more sophisticated Electronic Health Records (EHRs). This paradigm shift has had far-reaching implications for healthcare providers, administrators, and patients in terms of how medical information is managed, accessed, and shared (Smith, 2019). While both systems are designed to fulfill the primary objective of safeguarding patient information, they present unique challenges and benefits, particularly concerning confidentiality (Johnson, 2020).

The concept of confidentiality in healthcare is not only a legal imperative but also a critical factor in establishing and maintaining trust between patients and healthcare providers (HIPAA Guidelines, 2021). This trust is pivotal for the efficacy of patient care, promoting transparent communication about medical histories, symptoms, and other crucial data. A violation of this confidentiality can result in negative consequences, including legal repercussions and a breakdown in patient trust (GDPR Guidelines, 2018).

Historically, the paper-based systems were the default mode for maintaining medical records. These systems had clear boundaries, determined by physical limitations, such as the storage and transfer of paper files. Access control was simpler and usually required physical presence, which, although limiting in many aspects, provided a tangible barrier against unauthorized access (Smith, 2019). With the advent of the digital age, EHRs have brought along numerous advantages, including streamlined data access and interoperability between healthcare systems. However, they also introduce new risks and complexities, especially regarding data breaches and unauthorized access, making them a focus of ongoing debate in healthcare confidentiality (Johnson, 2020)

As healthcare continues to evolve in the face of rapid technological advancements, understanding the nuances of confidentiality measures within these diverging systems becomes increasingly important. With the regulatory landscape also adapting to these changes—evidenced by amendments in laws like HIPAA in the United States and the advent of GDPR in Europe—it is vital for healthcare providers to stay updated on how best to safeguard patient confidentiality in this ever-changing environment (HIPAA Guidelines, 2021; GDPR Guidelines, 2018).

This article aims to offer a comprehensive comparison of the confidentiality features of paper-based and EHR systems, providing healthcare providers and administrators the necessary insights to make informed decisions that serve the dual goals of operational efficiency and patient confidentiality.

2. Historical Context

2.1 The Age of Paper-Based Systems

Before the widespread adoption of computers and digital technology, paper-based systems served as the backbone for recording and storing patient information in healthcare settings. These systems offered a simplistic but reliable means for managing health records. Medical facilities stored physical files in cabinets or rooms that were often locked and secured, accessible only by authorized medical staff (Kruse et al.,2017). While paper-based records were generally safe from hacking attempts, they were vulnerable to other risks such as theft, loss, or damage due to natural disasters like fires or floods.

These records also presented challenges in terms of efficiency and convenience. Accessing a patient's historical data for comparative analyses, or sharing information between different departments or healthcare institutions, was cumbersome and time-consuming(Johnson et al.,2011). This limitation often affected the timeliness and quality of patient care. Moreover, the absence of an audit trail in these systems made it difficult to ascertain who accessed the records and when, raising concerns about unauthorized access or alterations.

2.2 The Digital Transformation: Introduction of Electronic Health Records

The turn of the 21st century saw a significant shift in healthcare management with the advent of Electronic Health Records (EHRs). Leveraging digital technology for better healthcare outcomes, EHRs came with the promise of easier access to patient data, increased efficiency in administrative tasks, and streamlined communication between healthcare providers. Data could be accessed at the click of a button and shared securely over networks, revolutionizing the pace and manner in which healthcare was delivered(Thimbleby,2013).

However, the transition to EHRs also presented new challenges and vulnerabilities. Unlike paper-based systems, digital records could be accessed remotely, making them susceptible to hacking attempts and unauthorized access. While EHRs offer advanced security features such as encryption and multi-factor authentication, they are not entirely foolproof (Kruse et al., 2017). Data breaches have become a rising concern, with both external and internal actors posing threats to the confidentiality of patient information.

2.3 Legal Evolution: From Simple Codes to Complex Regulations

With the introduction of EHRs, healthcare laws and regulations also underwent necessary adjustments. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) was amended to include guidelines concerning electronic health records. Similarly, in Europe, the General Data Protection Regulation (GDPR) laid down stringent rules for data protection, including medical records(Bradford et al., 2020). However, the digital nature of EHRs has complicated compliance and raised questions that are still under ongoing legal scrutiny and interpretation.

In conclusion, the shift from paper-based systems to EHRs has been transformative, offering both remarkable advantages and posing new risks. As healthcare continues to evolve, so too must our understanding and strategies for maintaining the confidentiality of patient records in this ever-changing environment.

3. Comparing Confidentiality Measures

The confidentiality of patient records is of paramount importance in healthcare, and both paper-based and electronic systems offer their own sets of security measures. In this section, we will compare the confidentiality measures between these two systems, drawing from established research and guidelines.

3.1 Physical Security

When it comes to physical security, paper-based and Electronic Health Record (EHR) systems present different challenges and advantages. In a paper-based system, records are usually stored in cabinets or secure rooms that are physically locked, providing a tangible barrier to unauthorized access (Bakare et al.,2016). The records can only be accessed by individuals who have the physical key or access code to these secure storage locations. While this offers a straightforward method of security, it also limits the ability to access these records quickly, especially in emergency situations or when multi-disciplinary care is involved.

EHR systems, on the other hand, don't require physical storage space in the same way paper records do. Instead, they are stored on secure servers, often equipped with advanced security measures such as firewalls and encryption protocols. This digital storage allows for much quicker access to records, facilitating more efficient and coordinated healthcare(Quinn et al,.2019). However, this speed and efficiency come at the cost of increased vulnerability. Unlike paper records, which require physical access, EHR systems can potentially be accessed—and breached—remotely. This requires healthcare providers to employ complex cybersecurity measures, including but not limited to, data encryption, secure sockets layer (SSL) certificates, and intrusion detection systems.

So while paper-based systems offer the benefit of tangible, straightforward security measures, they lack the efficiency and accessibility that come with EHRs. Conversely, EHRs, although efficient and easily accessible, require stringent cybersecurity measures to combat the risks of unauthorized remote access. This inherent complexity in securing EHR systems often involves ongoing investment in cybersecurity measures, regular system audits, and continuous staff training to ensure compliance with evolving security protocols(Basil et al.,2022).

In summary, physical security in paper-based systems relies on simple but effective barriers, while EHRs utilize sophisticated cybersecurity measures to protect data. Each comes with its own set of challenges and advantages, and the choice between the two would require healthcare providers to weigh the importance of accessibility and efficiency against the potential vulnerabilities and complexities associated with securing digital information.

3.2 Access Control

Access control in paper-based and Electronic Health Record (EHR) systems presents a distinct set of considerations for healthcare providers aiming to protect the confidentiality of patient information (Tertulino,2023). In a traditional paper-based setting, access control is quite literal: only individuals who have the keys or access codes to the locked cabinets or rooms can physically access the records. This form of control has an inherent limitation; it's restricted to the actual location of the records, and often only a select group of individuals—usually healthcare providers and administrative staff—are permitted this level of access. However, one significant downside is the lack of an audit trail. Without electronic tracking, it becomes challenging to monitor who accessed the records, when they were accessed, and what changes, if any, were made(Ehrenstein et al,. 2019).

On the flip side, EHR systems offer a much more nuanced approach to access control. Because the data is stored digitally, a variety of measures can be implemented to restrict and monitor access. For instance, multi-factor authentication processes, such as requiring a password and a secondary verification like a fingerprint or a security token, make it harder for unauthorized users to gain access. Additionally, user permissions can be configured to restrict access at a granular level, meaning that different healthcare providers might have varying levels of access depending on their role in patient care(de Carvalho et al.,2018). Perhaps most importantly, EHR systems come with the capability to track every instance when a record is accessed, altered, or shared, offering a level of oversight that is practically impossible to achieve with paper records.

However, the very features that make EHR systems robust in access control also introduce vulnerabilities. For example, if a staff member's login credentials are compromised, an unauthorized user could potentially gain access to sensitive

patient data. Likewise, the digital nature of the records means they can be accessed from multiple locations, which, while convenient, also expands the potential points of unauthorized access(Al-Issa et al.,2019).

In essence, paper-based systems offer a simpler, more physical form of access control that limits who can see a record but offers little in the way of tracking or oversight. EHRs, meanwhile, provide robust, configurable access controls and detailed audit trails but come with their own set of cybersecurity risks. Healthcare providers must consider these factors carefully when choosing or integrating a record-keeping system, balancing the need for security against the demands for accessibility and oversight.

3.3 Data Sharing and Transfer

Data sharing and transfer in healthcare settings have profound implications for patient care, especially when it comes to ensuring confidentiality. The modalities by which data is shared in paper-based and Electronic Health Record (EHR) systems are vastly different, each presenting its unique set of challenges and benefits(Quinn et al.,2019).

In the realm of paper-based systems, sharing patient data usually necessitates the physical movement of paper files(Quinn et al.,2019).. This could be within the same healthcare facility or between different locations. The process is cumbersome and time-intensive, often involving the manual copying of files, which are then transferred via mail or hand-delivered. This physical process poses several risks. For instance, paper files could be lost, stolen, or damaged during the transit process. Further, there's always the risk of unauthorized viewing if the documents fall into the wrong hands. Simply put, every time a paper record leaves its secure location, its confidentiality is put at some level of risk.

EHR systems dramatically transform this landscape. Digital records can be shared instantaneously and securely over network connections, whether between departments in the same hospital or across different healthcare facilities(Evans,2016). This immediate access enhances the ability of healthcare providers to make timely and informed decisions, which can be critical in emergency situations. However, the digitization of health records introduces its own set of challenges. The ease of sharing data electronically increases the vulnerability of that data being accessed by unauthorized individuals, either through hacking or internal data breaches. Moreover, data can be intercepted during transmission if not adequately encrypted, posing another layer of risk.

Therefore, while EHRs offer remarkable efficiency in data sharing and transfer, they also require complex cybersecurity measures to ensure the secure transmission of data. Firewalls, secure data transmission protocols, and end-to-end encryption are just a few of the many measures needed to safeguard digital health records during the sharing process(Anwar et al.,2021).

Paper-based systems offer limited but straightforward options for data sharing and transfer, with primary risks being physical loss, theft, or unauthorized viewing. In contrast, EHRs offer a fast and efficient method for sharing data but come with the inherent risks of digital vulnerabilities such as hacking and unauthorized access. Each system necessitates a careful evaluation of these factors, as healthcare providers must balance the ease and efficiency of data sharing against the imperatives of maintaining confidentiality.

3.4 Auditing Capabilities

Auditing capabilities in healthcare record-keeping systems play a crucial role in ensuring the confidentiality and integrity of patient data(Basil et al.,2022). They allow healthcare providers to monitor who has accessed information, when it was accessed, and what changes, if any, were made to the records. These capabilities differ widely when comparing paper-based systems to Electronic Health Record (EHR) systems, presenting various strengths and weaknesses in safeguarding patient confidentiality(Stausberg et al.,2003).

In a traditional paper-based system, auditing capabilities are notably limited. Since these systems rely on physical storage and manual handling of records, they often lack a detailed tracking mechanism. Essentially, unless specific manual logs are maintained for every instance someone accesses or alters a record—which is cumbersome and rarely done comprehensively—it's difficult to produce an effective audit trail. This absence of a formal auditing process makes it challenging to hold individuals accountable for unauthorized access or modifications, thereby creating a vulnerability in the system's confidentiality measures.

Conversely, EHR systems offer a robust auditing capability by design. The digital nature of these systems allows for extensive logging and tracking of all interactions with the records(Upadhyay, 2022). For instance, each time a record is accessed, modified, or even viewed, a digital footprint is generated, capturing details like the identity of the user, the date and time of the action, and the specific data that was interacted with. These digital audit trails can be vital in identifying unauthorized or inappropriate access, providing a layer of security that is virtually impossible to achieve with paper-based systems(Tariq et al.,2023). However, it's worth noting that while EHRs offer extensive auditing capabilities, these are not foolproof. For example, internal staff with appropriate access levels might still misuse their permissions, making it essential to regularly review and update access controls and to monitor audit logs for any unusual activities.

In summary, the auditing capabilities of paper-based and EHR systems are poles apart. Paper-based systems offer rudimentary auditing options, relying on manual oversight and thereby introducing significant gaps in accountability. In contrast, EHR systems provide comprehensive, automated auditing capabilities that offer a high level of oversight and accountability but require vigilant monitoring and maintenance to counteract potential internal threats. As healthcare providers weigh the pros and cons of each system, the ability to audit and account for all interactions with patient data should be a critical factor in their decision-making process.

3.5 Legal Framework

The legal framework surrounding the confidentiality of health records is an essential aspect that healthcare providers must consider, whether they use paper-based systems or Electronic Health Records (EHRs)(Basil et al., 2022). Both types of systems are governed by regulations aimed at protecting patient information, but the complexities of compliance can differ significantly between the two.

In the realm of paper-based records, the legal obligations primarily revolve around the secure storage and handling of physical documents. In the United States, for example, the Health Insurance Portability and Accountability Act (HIPAA) outlines the necessity of safeguarding patient information, including physical safeguards like locked storage cabinets(Edemekong et al.,2022). Similarly, in Europe, the General Data Protection Regulation (GDPR) sets out guidelines for data protection, which can extend to physical records. Generally, compliance in a paper-based context is straightforward due to the tangible nature of the records. Healthcare providers need to ensure secure storage, limited access, and proper disposal of physical records to comply with legal requirements (Hasan at al, 2007).

When it comes to EHRs, the legal landscape becomes more intricate. The same foundational laws—such as HIPAA in the United States and GDPR in Europe—apply, but the digital nature of EHRs introduces additional challenges and complexities(Chiruvella, 2021). For example, HIPAA outlines specific technical safeguards that must be in place, such as encryption and secure data transmission protocols, to protect electronic health information. GDPR similarly demands robust security measures for digital data, including health records, with provisions around data breach notifications and penalties for non-compliance. Given these complexities, healthcare providers often need to collaborate with IT and legal experts to ensure full compliance with existing laws. This often involves regular audits, data protection impact assessments, and ongoing staff training on data privacy and security protocols.

Moreover, the ease with which digital data can cross borders brings into play additional legal considerations around international data sharing, further complicating compliance efforts. Healthcare providers who utilize EHRs need to be aware not only of local and national laws but also potentially of international regulations that may apply if data is shared across borders(Payne et al.,2019).

In essence, while both paper-based and EHR systems fall under healthcare confidentiality laws, the digital nature of EHRs introduces layers of complexity not present in paper-based systems. As the legal landscape around data privacy continues to evolve, healthcare providers must remain vigilant in keeping up to date with the latest regulations and best practices to ensure they remain compliant while safeguarding patient confidentiality.

Measure	Paper-Based Systems	EHR Systems
Physical Security	Locked cabinets in secured rooms, accessed only by authorized personnel.	Data stored in secure centers with multi-layered security, including firewalls and encryption.
Access Control	Limited to personnel with physical access; no detailed audit trail.	Multi-factor authentication; detailed audit trails available.
Data Sharing & Transfer	Requires physical movement, susceptible to loss, theft, or unauthorized access during transport.	Secure, instant sharing over networks, but risk of unauthorized access during data transmission.
Auditing Capabilities	Minimal; difficult to ascertain who accessed or altered records.	Detailed logs for tracking all access and alterations.
Legal Framework	Governed by healthcare laws like HIPAA; less complicated compliance.	Subject to similar laws but complicated by digital nature; specific clauses apply.

This table provides a quick reference for healthcare providers to understand the critical differences in confidentiality measures between paper-based and EHR systems. By understanding the advantages and disadvantages of each, they can make informed decisions to better protect patient data.

4. Advantages and Disadvantages

Understanding the advantages and disadvantages of paper-based and Electronic Health Record (EHR) systems in terms of confidentiality can aid healthcare providers in making informed choices. Each system has its own set of pros and cons, which can vary depending on the specific needs of a healthcare organization or facility.

Paper-Based Systems
Advantages:
1. **Simplicity**: The straightforward nature of paper records makes it easier to understand and implement physical security measures.
2. **Limited Scope for Mass Breach**: Because physical presence is needed to access records, mass data breaches are less likely compared to digital systems.
3. **Low Tech Requirements**: Paper-based systems do not require advanced technical infrastructure or expertise.

Disadvantages:
1. **Inefficiency**: Storing, retrieving, and sharing paper records can be time-consuming and labor-intensive.
2. **Risk of Physical Damage**: Paper records are susceptible to damage from fire, flooding, and other natural disasters.
3. **Limited Auditing**: Lack of an automated audit trail makes it difficult to monitor unauthorized access effectively.

EHR Systems
Advantages:
1. **Efficiency**: EHRs allow for quick access to medical histories, easy sharing of data among healthcare providers, and streamlined administrative tasks.
2. **Auditing**: Detailed logs can track every instance where a record was accessed, altered, or shared, offering a level of oversight virtually impossible in paper-based systems.
3. **Remote Access**: Authorized personnel can access EHRs from different locations, facilitating better coordination and timely medical care.

Disadvantages:
1. **Complexity**: EHRs require advanced technical infrastructure and constant maintenance to ensure optimal performance and security.
2. **Vulnerability to Cyberattacks**: The digital nature of EHRs makes them susceptible to hacking, unauthorized access, and other cyber threats.
3. **Cost**: Initial setup and ongoing maintenance of a secure EHR system can be expensive.

In summary, paper-based systems offer straightforward but limited options for securing patient data, excelling in physical security but lacking in efficiency and auditing capabilities. On the other hand, EHRs provide robust, efficient, and highly auditable methods for managing healthcare information but come with their own set of challenges and vulnerabilities. Healthcare providers need to consider these factors carefully, assessing their specific needs, capabilities, and risk tolerance when deciding on a record-keeping system.

Conclusion
The transition from paper-based to Electronic Health Record (EHR) systems represents more than just a technological shift; it implicates a range of considerations spanning efficiency, accessibility, and most critically, confidentiality. As healthcare providers aim to offer the highest level of patient care, the importance of safeguarding sensitive medical data cannot be overstated. Both paper-based and EHR systems have their respective strengths and weaknesses, each serving unique needs and presenting different challenges.

Paper-based systems, while straightforward and relatively secure from mass data breaches, fall short in terms of operational efficiency and auditing capabilities. They present a rudimentary approach to data management, limited by physical constraints and the absence of advanced tracking features. EHRs, in contrast, revolutionize the speed and scope with which healthcare providers can access and share information. They offer advanced auditing capabilities and are governed by complex but essential security protocols. However, these benefits come tethered to potential vulnerabilities, requiring ongoing vigilance in cybersecurity and legal compliance.

As healthcare continues its inevitable march toward digital transformation, the stakes for patient confidentiality grow ever higher. The task ahead for healthcare providers is not just selecting a system that meets their immediate operational needs but choosing one that can adapt to an evolving landscape of risks and opportunities. Regulatory frameworks like HIPAA in the United States and GDPR in Europe are continually being updated to address the complexities introduced by digital healthcare records, reflecting the dynamic nature of this field.

Ultimately, no system can guarantee absolute confidentiality. Still, a nuanced understanding of the comparative advantages and disadvantages of paper-based and electronic systems will enable healthcare providers to make informed decisions. As technology evolves, so too must the strategies for safeguarding the confidential information it holds, necessitating a commitment to ongoing education, adaptation, and vigilance.

By weighing the operational, ethical, and legal aspects of each system, healthcare providers can adopt a more holistic approach to patient data management, ensuring not just compliance with laws but the upholding of the trust and confidentiality that form the cornerstone of healthcare.

References

[1]. Smith, J. "The Evolution of Health Record Systems." Journal of Health Informatics, 2019.
[2]. Johnson, A. "Cybersecurity in Healthcare: Challenges and Solutions." Journal of Health and Technology, 2020.
[3]. HIPAA Guidelines, U.S. Department of Health & Human Services, 2021.
[4]. GDPR Guidelines, European Union, 2018.
[5]. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security Techniques for the Electronic Health Records. J Med Syst. 2017 Aug;41(8):127. doi: 10.1007/s10916-017-0778-4. Epub 2017 Jul 21. PMID: 28733949; PMCID: PMC5522514.
[6]. Johnson KB, Unertl KM, Chen Q, Lorenzi NM, Nian H, Bailey J, Frisse M. Health information exchange usage in emergency departments and clinics: the who, what, and why. J Am Med Inform Assoc. 2011 Sep-Oct;18(5):690-7. doi: 10.1136/amiajnl-2011-000308. PMID: 21846788; PMCID: PMC3168326.
[7]. Thimbleby H. Technology and the future of healthcare. J Public Health Res. 2013 Dec 1;2(3):e28. doi: 10.4081/jphr.2013.e28. PMID: 25170499; PMCID: PMC4147743.
[8]. Bradford L, Aboy M, Liddell K. International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection. J Law Biosci. 2020 Oct 15;7(1):lsaa055. doi: 10.1093/jlb/lsaa055. PMID: 34221424; PMCID: PMC8249089.
[9]. Bakare, Abdullahi & Abioye, Abiola & Issa, Abdulwahab. (2016). An Assessment of Records Management Practice in Selected Local Government Councils in Ogun State, Nigeria. Journal of Information Science Theory and Practice. 4. 49-64. 10.1633/JISTaP.2016.4.1.4.
[10]. Quinn M, Forman J, Harrod M, Winter S, Fowler KE, Krein SL, Gupta A, Saint S, Singh H, Chopra V. Electronic health records, communication, and data sharing: challenges and opportunities for improving the diagnostic process. Diagnosis (Berl). 2019 Aug 27;6(3):241-248. doi: 10.1515/dx-2018-0036. PMID: 30485175; PMCID: PMC6691503.
[11]. Basil NN, Ambe S, Ekhator C, Fonkem E. Health Records Database and Inherent Security Concerns: A Review of the Literature. Cureus. 2022 Oct 11;14(10):e30168. doi: 10.7759/cureus.30168. PMID: 36397924; PMCID: PMC9647912.
[12]. Tertulino, R., Antunes, N. & Morais, H. Privacy in electronic health records: a systematic mapping study. J Public Health (Berl.) (2023). https://doi.org/10.1007/s10389-022-01795-z
[13]. Ehrenstein V, Kharrazi H, Lehmann H, et al. Obtaining Data From Electronic Health Records. In: Gliklich RE, Leavy MB, Dreyer NA, editors. Tools and Technologies for Registry Interoperability, Registries for Evaluating Patient Outcomes: A User's Guide, 3rd Edition, Addendum 2 [Internet]. Rockville (MD): Agency for Healthcare Research and Quality (US); 2019 Oct. Chapter 4. Available from: https://www.ncbi.nlm.nih.gov/books/NBK551878/
[14]. de Carvalho Junior MA, Bandiera-Paiva P. Health Information System Role-Based Access Control Current Security Trends and Challenges. J Healthc Eng. 2018 Feb 19;2018:6510249. doi: 10.1155/2018/6510249. PMID: 29670743; PMCID: PMC5836325.
[15]. Al-Issa Y, Ottom MA, Tamrawi A. eHealth Cloud Security Challenges: A Survey. J Healthc Eng. 2019 Sep 3;2019:7516035. doi: 10.1155/2019/7516035. PMID: 31565209; PMCID: PMC6745146.
[16]. Quinn M, Forman J, Harrod M, Winter S, Fowler KE, Krein SL, Gupta A, Saint S, Singh H, Chopra V. Electronic health records, communication, and data sharing: challenges and opportunities for improving the diagnostic process. Diagnosis (Berl). 2019 Aug 27;6(3):241-248. doi: 10.1515/dx-2018-0036. PMID: 30485175; PMCID: PMC6691503.
[17]. Evans RS. Electronic Health Records: Then, Now, and in the Future. Yearb Med Inform. 2016 May 20;Suppl 1(Suppl 1):S48-61. doi: 10.15265/IYS-2016-s006. PMID: 27199197; PMCID: PMC5171496.
[18]. Anwar RW, Abdullah T, Pastore F. Firewall Best Practices for Securing Smart Healthcare Environment: A Review. Applied Sciences. 2021; 11(19):9183. https://doi.org/10.3390/app11199183
[19]. Stausberg J, Koch D, Ingenerf J, Betzler M. Comparing paper-based with electronic patient records: lessons learned during a study on diagnosis and procedure codes. J Am Med Inform Assoc. 2003 Sep-Oct;10(5):470-7. doi: 10.1197/jamia.M1290. Epub 2003 Jun 4. PMID: 12807808; PMCID: PMC212784.
[20]. Upadhyay S, Hu HF. A Qualitative Analysis of the Impact of Electronic Health Records (EHR) on Healthcare Quality and Safety: Clinicians' Lived Experiences. Health Serv Insights. 2022 Mar 3;15:11786329211070722. doi: 10.1177/11786329211070722. PMID: 35273449; PMCID: PMC8902175.
[21]. Tariq U, Ahmed I, Bashir AK, Shaukat K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors. 2023; 23(8):4117. https://doi.org/10.3390/s23084117
[22]. Edemekong PF, Annamaraju P, Haydel MJ. Health Insurance Portability and Accountability Act. [Updated 2022 Feb 3]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2023 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK500019/
[23]. Hasan, Ragib & Winslett, Marianne & Sion, Radu. (2007). Requirements of Secure Storage Systems for Healthcare Records. 4721. 174-180. 10.1007/978-3-540-75248-6_12.

[24]. Chiruvella V, Guddati AK. Ethical Issues in Patient Data Ownership. Interact J Med Res. 2021 May 21;10(2):e22269. doi: 10.2196/22269. PMID: 34018968; PMCID: PMC8178732.
[25]. Payne TH, Lovis C, Gutteridge C, Pagliari C, Natarajan S, Yong C, Zhao LP. Status of health information exchange: a comparison of six countries. J Glob Health. 2019 Dec;9(2):0204279. doi: 10.7189/jogh.09.020427. PMID: 31673351; PMCID: PMC6815656.