Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 2 (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Privacy and Security of Medical Records in e-healthcare Environment System

Dr. Sanjay Kumar[1], Dr. Navin Kumar[2]

[1]Department of Computational Sciences, Brainware University, Kolkata, West Bengal

Email ID: dsk.cs@brainwareuniversity.ac.in

[2]Department of Law, Brainware University, Kolkata, West Bengal

Cite this paper as: Dr. Sanjay Kumar, Dr. Navin Kumar, (2025) Privacy and Security of Medical Records in e-healthcare Environment System. *Journal of Neonatal Surgery*, 14 (2), 274-280.

ABSTRACT

Several countries, including the United States, Great Britain, Australia, France, and Germany, are developing an efficient architecture and mechanism for the confidential exchange of medical data while maintaining patient privacy[1]. A growing number of healthcare organizations are implementing electronic health records (EHR) to eliminate paper use gradually.

Healthcare organizations and professionals' benefit from online access to patient records and diagnostic transactions. Furthermore, it raises serious concerns regarding privacy issues relating to the private data of patients, e.g., patients do not want their private health information to be known since this may harm their reputation or create problems for their careers.

Keywords: *Privacy, Security, Medical records, Patient, Environments...*

1. INTRODUCTION

EHRs that operate over the internet enhance patient access to their medical history anytime, anywhere. So, security and privacy become essential. In order to adapt an EHR, it is important to consider financial incentives, laws and regulations, conditions within the organization, and organizational influences [2].

The healthcare information system consists of following correlated records.

- Personal Health Records (PHR) are records that patients maintain themselves. Information from EMR and EHR is gathered to provide a complete summary of medical history.
- Electronic medical records (EMRs) can be created, used, and maintained by healthcare professionals to document, monitor, and manage healthcare services.

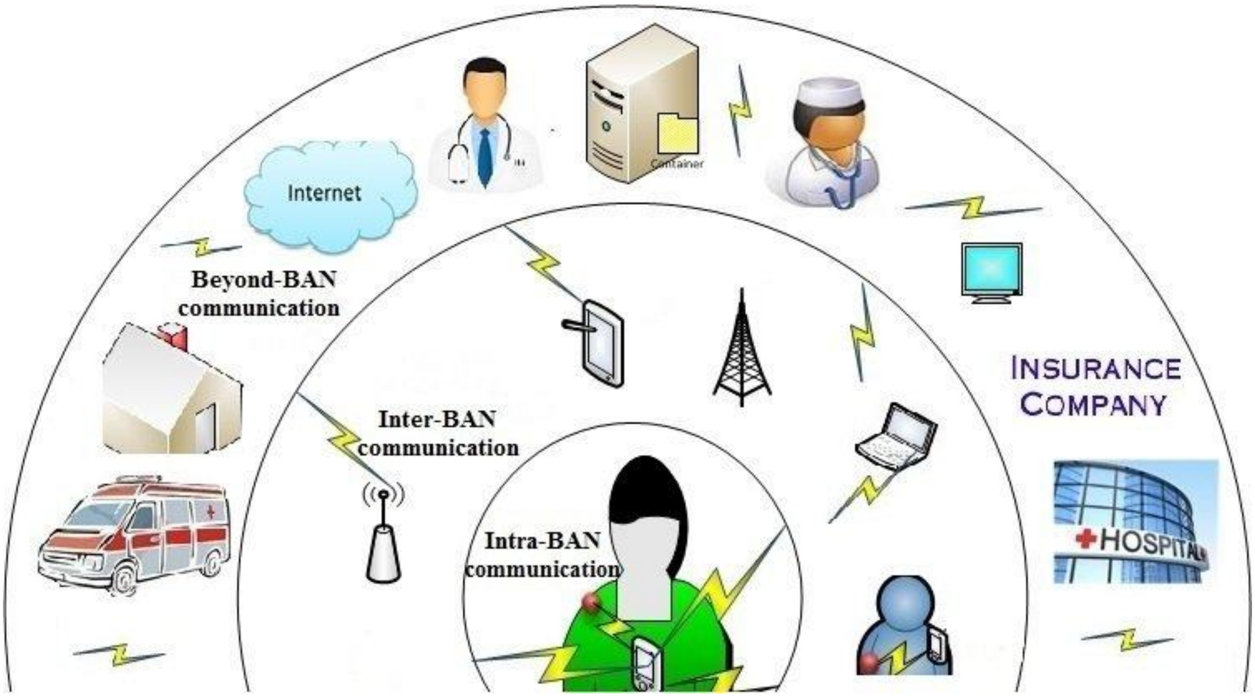

Figure1: healthcare environment system

In the United States, electronic health records (EHR) are maintained by the patient, are a subset of the EMR, and are created by the patient. A patient-involved EHR can be adapted for use across multiple healthcare delivery providers within a community.

It is highly desired that electronic health record systems integrate all relevant healthcare information of an individual and document their health history for life. In addition to insider threats, outsider intrusion into medical information systems is a crucial threat to healthcare information privacy[3]. These threats originate from the healthcare institution, from the secondary user setting, shown in figure 1.

Disclosure by an insider, insider curiosity, and insider subornation are all possible threats to confidentiality inside patient care institutions. Access by unauthorized individuals must be carefully monitored.

In general, deterrents, obstacles, and management precautions are three technological interventions that improve system security [4]. In order for deterrents to work, they must rely on people's ethical behavior and make sure they are reminded and overseen to maintain those standards. Directly limiting access to information, obstacles restrict a person's ability to access that information only to the extent they need to know it.

By proactively analyzing a system for vulnerabilities, systems management precautions ensure that vulnerabilities can be eliminated through known avenues.

2. SECURITY AND PRIVACY ISSUES

EHRs are associated with risks, so it is vital to ensure patients' privacy. When patients or healthcare providers access or transact with EHRs, the following security issues need to be appropriately addressed.

User Authentication

The user authentication process ensures that only authorized users have access to the health record when anyone attempts to access it. Several solutions using smart cards have been proposed. For ensuring authorized access to records, biometric systems are also used.

Confidentiality & Integrity

The topic refers to the accuracy and reliability of healthcare records and the integrity and dependability of physical computer and network systems. Data may be altered or clinical systems destroyed due to hacking incidents on EHRs[5].

Access Control

Medical records are stored in databases and exchanged via heterogeneous file systems in shared computing environments. This poses a security risk. Depending on how the system and organization are designed, it is critical to limit users' access to specific resources via granting or rejecting access to them.

It is effortless for an unidentified user to access a network if the remote connection to the network is not secure [12]. Electronic systems should enable core security features such as role-based access, passwords, and audit trails. The genetic testing process is fraught with privacy concerns. Many people are concerned about losing their jobs or their life insurance. Because genetic tests are ineffective, they hurt individuals, researchers, and physicians.

Data Ownership

Furthermore, the delegation of responsibility for accessing patient records is also essential. To whom will data be entrusted, and what is the delegation of authority? Furthermore, duties and responsibilities relating to data ownership should be transparent.

Data Protection Policies

As a result of the widespread involvement of multiple organizations and functions in healthcare diagnosis systems, reliable and consistent protection must be provided. Physical media and portable devices must be protected with strict policies and procedures to prevent loss or theft. To maintain security, add levels of security, prevent access to particular notes or results, track versioning, and mask sensitive entries, EHR systems need to develop new functionality continuously[6].

User Profiles:

Patients, practitioners, healthcare organizations, trusted third parties, pharmacists, etc., are involved in the healthcare system. As a result, defining user types and roles for defining user requirements and security levels has become increasingly important.

Identifying patients within and between healthcare facilities is complex due to the wide variation and incompatibility of patient identification systems. For interoperability to occur, patient IDs must be shared between entities. The industry presently does not have a standard for record-to-record matching[10].

Misuse of Health Record:

Some websites offering electronic health records, particularly those providing free storage space, are not concerned with privacy. The companies can sell the patient's data to other companies or advertise on the same web page where the patient uploaded content. Keeping health records secure can be difficult in a multispecialty setting. As patients treated for substance abuse tend to fall into multiple medical specialties, companies must separate any records that relate to their treatment.

Privacy in e-health is a difficult task compared to other fields as:

- The timing of data gathering may vary from day to week, and e-e-healthcare systems will learn about the everyday life of a patient;
- The obtained data are not only physiological but also conductual (i.e., dietary or everyday activities of the patient);
- Data collected are often transmitted between different divisions (e.g., health and research insurance); and
- Individual users, gender, ethnic and cultural groups all have different perspectives, interests, and privacy requirements.

Contemporary e-health research (2010-2015) has shown control of access and data confidentiality but overlooking other vital issues such as data protection, anonymity, and auditing. A recent study has also indicated that patients and users' safety problems with mobile phones and PDA interfaces need to be resolved. This requires platform safety and security through design and safety planning and development.[7]

Recent research has shown that interruptions in e-health companies have occurred because of the lack of established privacy and security rules. Unintentional data loss, delays to productivity, and challenges with operational feasibility [11] have led to little attention to and implementation of academic requirements. In addition to the lack of coordination between different actors and the lack of understanding of the whole spectrum of e-health enterprises, it has led to progress towards a more efficient-health sector.

3. USERS IN REMOTE LOCATIONS

Advancements have greatly influenced research on universal healthcare and remote monitoring of human activities and health in sensor technology, wearable computing, and the Internet of Things (IoT).

Various sensor, wearable, and smartphone-based health monitoring systems help monitor patients' psychological and health conditions by processing and analysing data. These systems enable continuous monitoring of patients' psychological and health conditions through monitoring their behaviours, shown in figure2.

The following major features (tiers) are included in each electronic health care system[13]:

- A centralized network that serves as a repository for all data and equipment,
- A body area network (BAN) collects data on a patient's health status.
- Users of the general pattern may be located remotely about the System's communication users (physician, pharmacist, e-healthcare insurance provider, etc.)

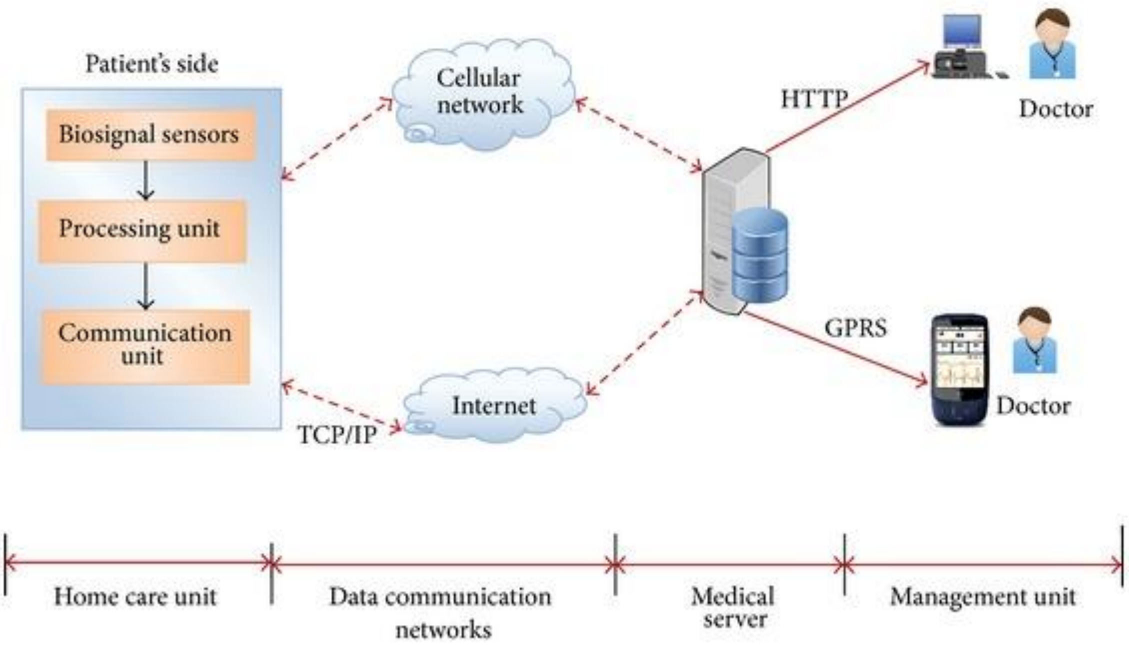

Figure2: e-healthcare data

3.1 Issues in Electronic e-healthcare

The merging of the ICT, IoT, and cloud technology ecosystems raises several problems. E-health companies must comply with several regulations, including legal limits (e.g., HIPAA). These are the key

As healthcare becomes more competent, it is becoming more important to use information and communication technology (ICT). Instead of keeping patient information within a written file, all information is organized in a database as well defined files that can be accessed through a specific system in almost every hospital. Some files got lost, or information was separated into separate files at different hospitals or departments, which meant no one could access the whole picture. With this in mind, we formulated our framework. This paper aims to keep that information available in the cloud so physicians and nurses can view patients' records from any place, so they are aware of their history, which helps doctors make the right decisions. E-Health privacy domains are developed through a security architecture. The user will be able to moderate their medical data and improve the availability of medical data. Also, e-Health has multiple components under attack in cloud computing.

Furthermore, we want to set out different types of hackers. We indicate several weaknesses in current e-Health solutions and standards, especially in client platform security, crucial in securing e-Health systems. This is addressed by presenting a privacy architecture for e-Health infrastructures. Our solution provides client and platform security to clients and networks in a compatible manner.[14]

While eHealth systems seek to improve the quality of e-Healthcare and save expenses, they also cause patients new challenges. These problems are “IoT, communication lines, cloud storage, and access control – a separate and merged e-health company”. Patients' information is highly private and protected, with a risk protection policy at all levels, from sensors to cloud storage[15]. There may be safe keep in fears to e-health framework. These can include architecture (sensors, PDAs, cloud, and communication), administration (minimal policies and access control), or natural software (application). Each component and layer of the electronic e-health system must be safeguarded.

The leading obstacle stays to build hardware for the patient to the hospital, i.e., “a WSN and a communication link”. Data transfer from a BAN sensor to the heart of an e-health system must be safe and fast. BAN communication to the leading network offers a range of security concerns and weaknesses. Its security goals are identical to any other component of e-health systems (such as privacy, integrity, and availability). Still, IoT-based risk perception and mitigation require exceptional understanding and management. Research on the management and compliance implications of the WSN and IoT is significantly lacking. To date, severe interoperability issues have developed for e-health providers without standards in an e-hygiene organization.

Another primary security concern is data protection during transmission or storage. Robust authentication techniques must be integrated into e-health systems using safe encryption technology. Most patients prefer to connect to their existing mobile phones with the BAN and core e-health networks instead of acquiring a device which is viable in terms of confidentiality. “The system, however, is exploiting common resources (smartphones, internet) and therefore subject to attacks its main flaws (applications, systems, and protocols)”. E-Health usually fails to save, share and access data on a server. Many operational organizations and servers already identify security approaches suitable for security, secrecy, and other e-health duties. However, many adjustments are needed to meet the unique functional and compliance needs of the e-health industry. Cloud technology's back-end use exacerbates this, making cloud-related difficulties an already complex e-healthcare enterprise.[16]

Perhaps the major obstacle to e-health providers building patient trust and integrating e-health systems is privacy. A typical patient may think that privacy is the only feature of e-health architecture, albeit not necessarily. The confidence gap between the Systeme and its users can be addressed by accessing and sharing health information by people.

4. PRIVACY AND SECURITY ON ACCESS CONTROL MODEL

Role-based access control (RBAC) restricts network access based on a person's role within an organization and has become one of the primary methods for advanced access control. Within RBAC, roles refer to access levels to employees' network.

Access to confidential information is restricted solely to employees who need it to perform their duties. The factors that determine access include authority, responsibility, and job competency. Further, access to computer resources can be restricted to particular tasks, such as seeing, creating, or editing documents, shown in figure3.

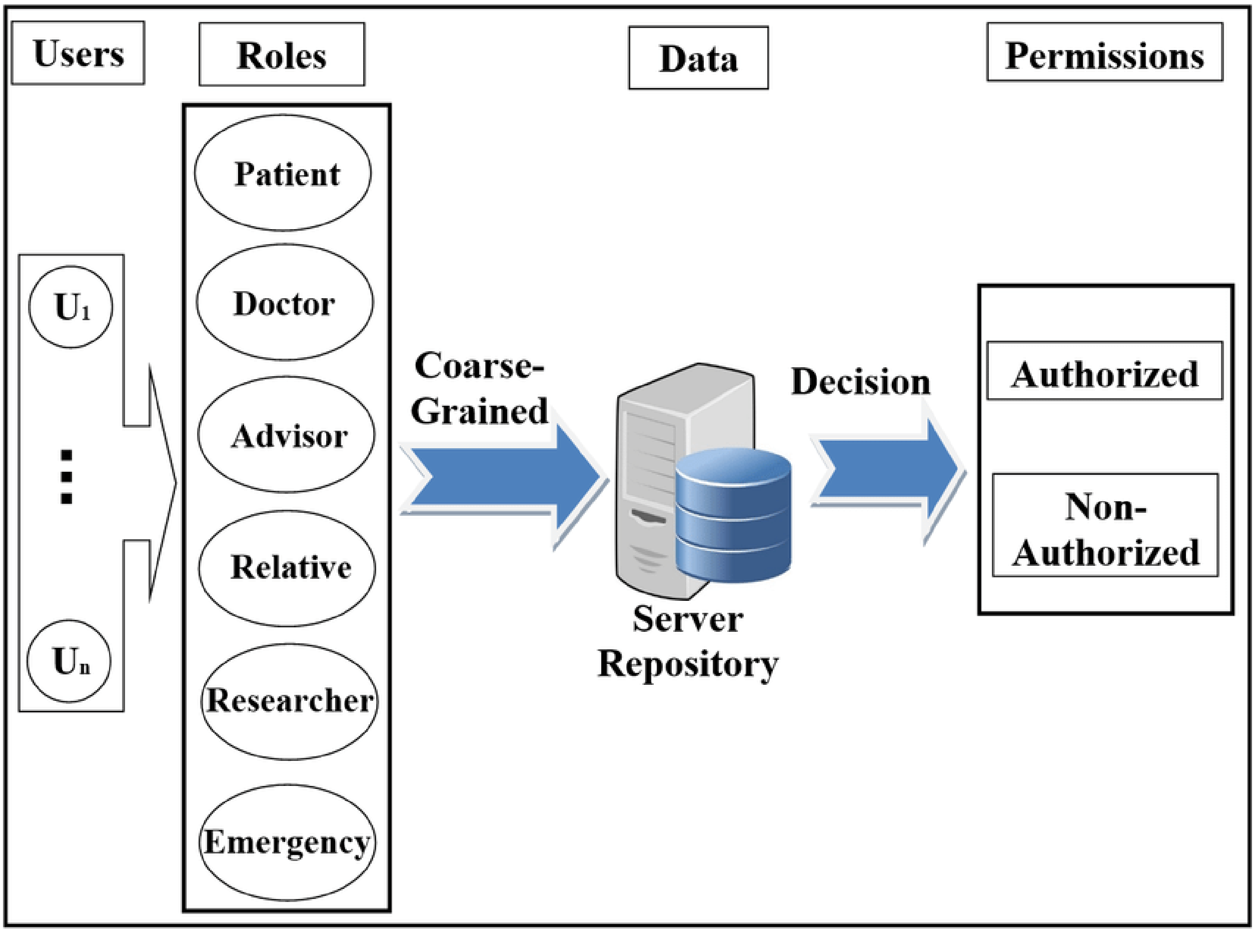

Figure3: Access control model

As a result, lower-level employees do not have access to sensitive data if they do not require it to perform their tasks. You will benefit from this if you have many employees and use contractors and third parties, making it difficult to monitor access to the network closely. Your company's sensitive data and essential applications must be protected through RBAC. The RBAC method allows you to configure both broad and granular permissions for end users. If your employees are assigned different roles and access permissions depending on their positions in your organization, you can identify whether they are administrators, specialists, or end-users. Upon granting access to employees, only the amount necessary to enable them to perform their duties is allowed.

How does this affect end-users whose jobs change? A role may need to be manually assigned to another user, a role can be assigned to a role group, or a role assignment policy can be used to add or remove members of a role group.

Conclusion

After analyzing the latest e-health privacy research, one approach was insufficient because all privacy concerns had not been addressed. To secure the privacy of e-health care, the specific characteristics must be understood. In how the e-health environment and the conditions of its patients are considered, privacy must be specified. The factors causing this scenario were the lack of a clear definition and understanding among the parties in global polls of privacy, regulation, interagency collaboration, and conflicting interests. In particular, data protection regulations should ensure that patients maintain their ownership of PHI/EHR. This work sums up existing research in this area and defines a high-level data protection system design that addresses all major privacy concerns. For such comprehensive and sophisticated use of single protocols, the subsequent abstract data protection architecture in e-healthcare should provide insufficient security and privacy.

REFERENCES

[1] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. 2002. Hippocratic databases. In *VLDB'02: Proceedings of the 28th International Conference on Very Large Databases*. Elsevier, 143–154.

[2] Raag Agrawal and Sudhakaran Prabakaran. 2020. Big data in digital healthcare: Lessons learnt and recommendations for general practice. *Heredity* 124, 4 (2020), 525–534.

[3] . M. Ahmed, E. Elaziz, and N. Mohamed. 2020. Nurse’s knowledge, skills, and attitude toward electronic health records. *Journal of Nursing and Health Science* 9 (2020), 53–60.

[4] . Tareq Ahram, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, and Ben Amaba. 2017. Blockchain technology innovations. In *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*. IEEE, 137–141.

[5] Jagmeet Singh Aidan, Harsh Kumar Verma, and Lalit Kumar Awasthi. 2017. Comprehensive survey on Petya ransomware attack. In *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*. IEEE, 122–125.

[6] . Sunday Adeola Ajagbe, A. O. Adesina, and J. B. Oladosu. 2019. Empirical evaluation of efficient asymmetric encryption algorithms for the protection of electronic medical records (EMR) on web application. *International Journal of Scientific and Engineering Research* 10, 5 (2019), 848–871.

[7] . D. Akarca, P. Y. Xiu, D. Ebbitt, B. Mustafa, H. Al-Ramadhani, and A. Albeyatti. 2019. Blockchain secured electronic health records: Patient rights, privacy and cybersecurity. In *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE, 108–111.

[8] . Mubeen Akhtar. 2024. Innovations in anesthesia delivery: Tailoring care to individual patient needs. *Cosmic Journal of Biology* 3, 1 (2024), 184–190.

[9] . Bassim Al Bahrani, Itrat Medhi, and Itrat Mehdi. 2023. Copy-pasting in patients’ electronic medical records (EMRs): Use judiciously and with caution. *Cureus* 15, 6 (2023).

[10] Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. 2019. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems* 95 (2019), 511–521.

[11] Abdullah Al Omar, Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto. 2017. MediBchain: A blockchain based privacy preserving platform for healthcare data. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10*. Springer, 534–543.

[12] . Hameed Hussain Almubarak, Mohamed Khairallah Khouja, and Ahmed Jedidi. 2022. Security and privacy recommendation of mobile app for Arabic speaking. *International Journal of Electrical & Computer Engineering (2088-8708)* 12, 5 (2022).

[13] . Muhammad Anshari. 2019. Redefining electronic health records (EHR) and electronic medical records (EMR) to promote patient empowerment. *IJID (International Journal on Informatics for Development)* 8, 1 (2019), 35–39.

[14] Guy Aridor, Yeon-Koo Che, and Tobias Salz. 2021. The effect of privacy regulation on the data industry: Empirical evidence from GDPR. In *Proceedings of the 22nd ACM Conference on Economics and Computation*. 93–94.

[15] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. 2016. MedRec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 25–30.

[16] W. Bani Issa, I. Al Akour, A. Ibrahim, A. Almarzouqi, S. Abbas, F. Hisham, and J. Griffiths. 2020. Privacy, confidentiality, security and patient safety concerns about electronic health records. *International Nursing Review* 67, 2 (2020), 218–230.