**Security and Privacy of Health Data**

Mikhail Nikov

ISSC431: Database Systems Security

American Public University System

July 18, 2021

# Abstract

The security and privacy of health information is an issue of growing concern in the healthcare industry. Technological advancements have led to the adoption of digital records in healthcare organizations. Besides, the increased regulations need for health data between physicians, patients, health consolidation and healthcare insurance companies are all directed to better information security. This research paper critically surveys the existing knowledge and research literature on healthcare information security and privacy. The healthcare information security and privacy literature are obtained from both information system and published non-information system disciplines. The primary information system disciplines used for this study include health informatics, information systems, medicine and other widespread reports on the healthcare sector. This survey provides a holistic view of the most recent studies on the security and privacy of patient’s health information. However, we also suggest that the researcher conduct more research on the new areas of interest related to information systems and the protection of patients’ medical data.

[Abstract 2](#_Toc79088703)

[Introduction 4](#_Toc79088704)

[2.0. Background 4](#_Toc79088705)

[3.0. Security and Privacy Issues 5](#_Toc79088706)

[3.1. User Authentication. 6](#_Toc79088707)

[3.2. Access Control 6](#_Toc79088708)

[3.3. Ownership of Data 7](#_Toc79088709)

[3.4. Data Protection Policies 8](#_Toc79088710)

[3.5. User profiles 9](#_Toc79088711)

[3.6. Misuse of database information 9](#_Toc79088712)

[4.0. Current trends on privacy and security of database systems 10](#_Toc79088713)

[4.1. Human error 10](#_Toc79088714)

[4.2. Hacking or malware 10](#_Toc79088715)

[4.3. Insiders 11](#_Toc79088716)

[5.0. Privacy and security solution in database systems 11](#_Toc79088717)

[5.1. Deploy physical database security 11](#_Toc79088718)

[5.2. Install separate database servers 12](#_Toc79088719)

[5.3. Avoid using default network ports. 12](#_Toc79088720)

[5.4. Use real-time database monitoring 13](#_Toc79088721)

[6.0. Conclusion 13](#_Toc79088722)

[References 15](#_Toc79088723)

# Introduction

Recent government programs support the implementation of universal electronic health records across the healthcare organizations. Information systems play an essential role to improve the quality of healthcare services and reducing medical costs. Inadequate security controls in healthcare databases may lead to data breaches. These data breaches, however, exposes patients to economic difficulties, mental anguish, and social stigma. Recent research carried out in the US suggests 75% of patients are more worried about websites that illegally share patients' data without their consent (Thapa & Camtepe, 2020). The primary reason for this concern is that healthcare data disclosure is the second-highest in reported data breaches. Researchers in healthcare information systems have adapted numerous reference disciplines in information security risk management. They use disciplines like sociology and psychology to analyze the roles of all individuals in information security risk management. Besides, they use these disciplines in economics to characterize investment decisions and healthcare information governance (Thapa & Camtepe, 2020). This research analyzes security and privacy of healthcare records as regards to patients. It illuminates comprehensive researches, each with different scope of confidentiality and security of healthcare data. The research focuses on security and privacy, data protection policies, security and privacy solutions in the databases and the current trends on confidentiality and security of the database systems.

**2.0. Background**

Healthcare Data privacy refers to the underlying principle that governs the relationship between the patient and the physician for effective delivery of quality healthcare. Patients should feel free to share their health information with their physicians to promote correct diagnosis. The data privacy principle facilitates the proper diagnosis and determination of treatment as it enables patients to freely share accurate health information with the physicians (Chenthara et.al., 2019). As a result, it minimizes the cases of adverse drug interactions. In most cases, patients refuse to reveal important health information such as HIV status to avoid social discrimination and stigma. Eventually, a patient’s medical records accumulate crucial information such as medical history, dietary habits, genetic information and physician’s subjective assessments of the patient’s personality. Researchers can use patients’ medical information in their studies to advance medical science. Healthcare organizations can send the medical data to healthcare insurance companies such as Medicare or Medicaid. This is usually meant to justify payment for hospital bills for medical services rendered. Patient’s health records help hospitals to manage their medical services and identify new chances to improve the quality of their services (Shakeel et. al., 2018). Also, healthcare providers can share patients’ health data with other regional healthcare clinics to make care services easier. Generally, patients’ medical data is used for common benefit by federal and state government interventions for accreditations of clinical institutions. The data also help government interventions to manage social welfare systems and public health..

**3.0. Security and Privacy Issues**

Data confidentiality involves the ability of healthcare facilities to protect patients’ sensitive data. It entails governance and use of patient’s identity and health information. Healthcare data privacy encompasses making policies that govern the collection and sharing of patient’s data (Keshta & Odeh, 2020). On the other hand, data security refers to the protection of personal health information against unauthorized access. Some of the data security protections include the explicit mention of data availability and integrity. Usually, healthcare data security focuses on the protection of patient’s health information from pernicious attacks and stealing of data (Wilkowska & Ziefle, 2012). Despite being vital for data protection, data security is significantly insufficient for addressing data security in the healthcare sector. The main confidentiality and protection issues are discussed as below:

**3.1. User Authentication.**

User authentication involves the confirmations of the validity of the claims made by the user to access an information system. Authentication is a critical function in the information systems of healthcare organizations as it secures access to the organizations' networks. It protects the identities of system users and ensures that the users are who they are pretending to be (Shakeel et. al., 2018). Information authentication attacks like the man-in-middle (MITM) attacks can cause crises in healthcare information systems. Healthcare organizations use cryptographic measures and controls, such as the transport layer security (TLS) and secure sockets layer (SSL) to protect their network communications. Another vital user authentication tool is the Bull eye algorithm. This algorithm help in monitoring all sensitive information in the healthcare databases. It is widely used to secure healthcare information and manage the patient's original and replicated data (Keshta & Odeh, 2020). The bull eye algorithm allows only the authorized person to access, read, or write critical healthcare information on the systems. Generally, healthcare information systems should always validate the identity information of service providers and patients before granting them access to the information systems.

**3.2. Access Control**

After the authentication, users can access the database systems to obtain medical records they need. However, the access to the databases is still managed by the access control policy which is based on the rights granted to the physician by the patient. The access control policy is a flexible and powerful means that permits users to access the information systems (Wilkowska & Ziefle, 2012). It offers the users with complex controls which only allow them to perform the tasks for which they have permission. For example, the users may be authorized to perform several tasks like cluster administration, job submissions and data access. In the health care system, several solutions such as Role-based and attribute-based access control help in addressing data security and access control issues(Keshta & Odeh, 2020). These are some of the most popular modes of electronic health record (EHR) models. Therefore, healthcare facilities should adopt technologies with security access controls and data encryption techniques. This helps them to satisfy the fine-grained access control while preserving patients’ data security and privacy.

**3.3. Ownership of Data**

Healthcare organizations tend to believe that they are the owners of the patients' data because they lead the duty of obtaining it from the patients. However, medical clinics are merely "data guardians" as the data they collect belongs to the patients. Physicians cannot access and use patient's data outside the clinic without the knowledge of the patients. As a result, all clinical institutes are limited to exploiting the "big data" in the clinical databases for scientific research. They are advised to always get patients' approval to collect and use these records in future scientific studies. The privacy rule under the HIPAA legislation and the PIPEDA of Canada gave more protection to patients’ data (Shakeel et. al., 2018). The GDPR and other related laws like the CCPA have taken patient's rights to own their medical data to another level as they do not sufficiently address the ownership of patients' medical records. However, these laws do not apply in countries outside the European Union. This makes it more justifiable for healthcare facilities to always have patient's consent before using their medical data for scientific research.

**3.4. Data Protection Policies**

A data protection policy refers to a statement that outlines how a healthcare organization protects personal data. It comprises of rules, principles, and guidelines that explain how the organization will constantly comply with data protection laws. Organizational policies are as important as technical procedures an organization uses to protect patient's privacy and electronic health data. These policies help the organization establish goals for technical mechanisms and outline automatic use and data release. The organization uses data protections policies to set rules for disciplining the offenders and create methods for detecting and preventing data violations. Policies and practices must balance patients' right to privacy against the need for physicians to access relevant health data during service provision (Wilkowska & Ziefle, 2012). This balance makes patients more willing to reveal sensitive health information to their healthcare providers. Healthcare institutions have adopted several formal policies to help them outline their goals while maintaining patient's privacy and security. These policies include the procedures related to exchanging health information, authorized uses, and patient-centered approaches. Examples include confidentiality policies, security policies, and policies on research uses of healthcare information (Keshta & Odeh, 2020). They are primarily intended to help the organization promote a stronger relationship between the physicians and the patients while maintaining patient privacy. The contents of data protection policies and the techniques used to develop them play a vital role in ensuring the employees stick to them. Generally, policy documents are very effective when they are made as ongoing reference materials and easily accessible to the service providers. Besides, they should be introduced to the employees at the start of the employment and regularly used in employee training.

**3.5. User profiles**

A user profile refers to a directory of installed user information and settings for related user accounts. For example, a user profile can have settings for the operating system and installed programs (Wilkowska & Ziefle, 2012). However, when a user profile is in an operating system, it is usually unique to the same operating system on which it is stored. In healthcare systems, a user profile can cover information accounts relating to healthcare insurance of the patients, public and private financing and overall healthcare spending. User profiles also provide an overview cover for health system organization, information governance, information relating to patients disparities and evidence-based practices of healthcare services (Keshta & Odeh, 2020). They help in protecting patients' health information that may involve a consideration attributable to the organization's overall security program. It involves necessary protection based on the type of healthcare information protected from access by third parties. 

**3.6. Misuse of database information**

Medical records in healthcare database systems can be misused unless they are protected from unauthorized users. Patients' identifying data, therefore, should be coded to ensure that they are hidden from any authorized users. If a patient has received treatment from a medical institution for a particular disease, their medical information should be confidential. Failure to protect such information, a company selling products relating to the condition can directly contact the patient (Keshta & Odeh, 2020). However, this may not pose a problem, but in some cases, the patient may not want the medical information to leak to the family members through their mail. An example of such a case is when the patient has received treatment for a sexually transmitted disease. Also, there are concerns about discrimination resulting from medical data to determine patients' eligibility for housing, employment, and other related services. In the United States, HIPAA's primary goal is to deal with such issues. The United States government enacted this legislation to address security and privacy issues surrounding personal medical data (Wilkowska & Ziefle, 2012). The Act required that physicians, healthcare givers and health plans implement privacy rules regarding health information. In 2001, the US Congress proposed an additional protection rule in at least three bills. The main objective of these bills was to prevent discrimination based on patient's genetic data concerning healthcare cover. 

**4.0. Current trends on privacy and security of database systems**

**4.1. Human error**

Human error is the most common cause of data breaches in any organization. However, it does not involve sophisticated security breaches, data corruption or hardware failures. As it goes, an old joke in information technology: the problems of human error exist between the chair and the Keyboard. This means that the human factor in the system is the cause of the issues a system experiences. In this case, data loss is no exception. Recent studies show that the percentage loss of data in health care organizations due to human error is around 25% (Thapa & Camtepe, 2020). Data loss due to human error can be reduced with proper training of service providers and installing security controls. Such measures would help healthcare organizations to secure their offsite backups and protect patient's medical records. 

**4.2. Hacking or malware**

It is not easy for healthcare organizations to ignore the increasing reports on hacking and malware victimization in healthcare systems. Hacking and malware have become a significant threat that MI-ISAC, FS-ISAC and NH-ISAC teamed up to train healthcare facilities how to defend against such threats. Hackers usually hack the hospitals' information systems to steal medical records to sell on the dark web (Thapa & Camtepe, 2020). Ransomware is one of the main types of malware that infest healthcare stems and files, making them inaccessible. Nobody, not even the physicians, can access the files stored in the healthcare systems unless the ransom is paid. In the case of Ransomware malware in the healthcare sector, most of the critical processes slow down. Ultimately, such operations may become inoperable. Hospitals can, therefore, be forced to go back to analogue ways to record patients' health information using pen and paper. Ultimately, the entire medical process slows down and may soak up some funds that could have been used to modernize the hospital facility. 

**4.3. Insiders**

In most cases, healthcare institutions tend to be obsessed with defending the integrity of their networks from external threats. Such obsessions helps the organization to address the risks that may lie within their insiders. An insider to a company's networks poses a security threat because it has legitimate access to proprietary systems (Keshta & Odeh, 2020). The legitimate access of the insiders to the healthcare system prevents them from facing traditional cybersecurity defaces, including physical security and intrusion detection. Besides, insiders may also have some knowledge of the organization's network vulnerabilities and setups. Usually, insider threats in healthcare systems encompass a range of employees, including those who unknowingly click on unsecured links, which may compromise the network. Moreover, such malicious links may make the healthcare facility lose a work device that stores sensitive health data to the cybercriminals.

**5.0. Privacy and security solution in database systems**

**5.1. Deploy physical database security**

Hospitals can protect their data centers and private servers from physical attacks by simply installing additional security controls. Usually, it is difficult for organizations to detect physical attacks by an insider or even outsider threats. Such attacks can easily bypass the digital security protocols and controls and allow cybercriminals to access organizations' physical database servers (Thapa & Camtepe, 2020). Healthcare organizations are therefore advised to install additional security measures such as multiple layers of independent systems. Such systems may include parameter intrusion detections, CCTV surveillance and deterrent systems. This would prevent cybercriminals from accessing the physical database servers to corrupt and steal the organization's medical records.

**5.2. Install separate database servers**

Databases systems should have security measures and controls to protect them from cybersecurity risks. Having the organizational data on the same database server as its site exposes it to all security vulnerabilities that target the websites. Healthcare organizations can use website security protocols provided by the hosting service to protect patients' medical records from cyber attacks (Keshta & Odeh, 2020). Nevertheless, their sensitive data in the same database servers and websites are always vulnerable to attacks from online platforms and the site itself. Any attack breach in the organization's website allows the cybercriminal to access the medical records in its databases. 

**5.3. Avoid using default network ports**

When setting up TCP and UDP protocols to transmit data between servers in healthcare facilities, they tend to use default network ports. Such ports are commonly used in brute force attacks because they occur from time to time. The use of non-default ports subjects the cyber attackers to try several times in their attempts to access the facilities' database systems (Thapa & Camtepe, 2020). Therefore, hospitals should avoid using such default ports to discourage cyber attackers from prolonging their attempts to attack the facilities' databases. However, it is essential for the organization to always check the port registry in Internet Assigned Number Authority. This ensures that the new port is not used for other services by another user. 

**5.4. Use real-time database monitoring**

The real-time monitoring of hospitals' databases involves an active scanning of their databases from security breach attempts. It allows the facility to react to all possible security vulnerabilities. Healthcare institutions should install monitoring software like Tripwire's real-time file integrity monitoring (FIM) in their databases (Shakeel et. al., 2018). This software would help the organization scan all database breaches and allow the organization to react to possible attacks. Also, healthcare organizations must set up escalation protocols to protect their sensitive information from all potential attacks. Auditing the database system is another aspect that allows the organization to discover security risks within its database systems and patch them before they occur.  

**6.0. Conclusion**

Healthcare system has grown from a patient-physician relationship dynamics to a complex network that links patients to various stakeholders in the healthcare sector. The adoption of the new technologies into the healthcare industry is, therefore, likely to improve the quality of healthcare services. Also, this transformation has dramatically influenced the reduction of healthcare costs and the advancements in medical science. Despite being advantageous to the entire industry, technological changes have negatively impacted the healthcare system. They have increased the risk of security and privacy violation of patients' health information. The growing digitization of health and medical records has led to rising cases of medical identity theft. In this research paper, we have discussed the security and privacy issues of medical records. We have reviewed the existing body of knowledge across several issues about the security and privacy of healthcare information. The review indicates that healthcare organizations should not disclose patients' medical records to third parties without their consent. Due to the increasing reliance on web-based systems in managing patients' medical records, patients' concerns have been given priority in security and privacy rules. However, future studies may be conducted on the variance in security and privacy preferences among different users in the context of online systems.

# 

# References

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access, 7, 74361-74382.

**Summary:** Chenthara, Ahmed, Wang, and Whittaker highlight the research problems and directions in cybersecurity so that a comprehensive security model for electronic healthcare records may be developed (EHR). They also go over several important challenges and the numerous potential for further research in EHR security and privacy. Because big data can give a wealth of knowledge and information in e-Health systems, important privacy and security issues must be addressed right away. Studies must concentrate on EHR security methods that are both practical and thorough and strategies for maintaining the confidentiality and integrity of patient data.

Keshta, I., & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal.

**Summary:** Keshta and Odeh's research focuses on the impact of technology in the storage of health data. They also review the concerns, the safety theme, or features that EHR systems should apply. Therefore, Researchers can better grasp these privacy and security problems and the remedies that are accessible as a result of the review.

Shakeel, P. M., Baskar, S., Dhulipala, V. S., Mishra, S., & Jaber, M. M. (2018). Maintaining security and privacy in health care system using learning based deep-Q-networks. Journal of medical systems, 42(10), 1-10.

**Summary:** This paper provides a research on the effective framework for maintain security and privacy of health information in the internet setting. It mentions various roles of healthcare place in the protection of medical data from internet vulnerabilities. Besides, it focuses on the role of Internet of Things in providing effective security protocols for protecting health information.

Thapa, C., & Camtepe, S. (2020). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine, 104130.

**Summary:** Thapa and Camtepe conducts an extensive research on the electronic health monitoring designs using computations, sensing technologies and communication. Their research paper provide various reasons why the security and privacy of health data should be given the first priority. For example, the information should be protected from third parties because if it leaks it would affect the personal life of a patient. Therefore, the security and privacy of the patients’ medical data is of high importance.

Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in E-health: Requirements from the user’s perspective. Health informatics journal, 18(3), 191-201.

**Summary:** This study focuses on two main aspects of using assistive technologies to enhance security and privacy of medical records. It specifically addresses the importance of security and privacy concerns in healthcare system in relation to health status, age and gender of the patients.