IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13427

DATA SECURITY AND PRIVACY MANAGEMENT IN HEALTHCARE

U. Ranjith[1], Dr S Shanthini[2]

Department of Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Department of Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: Health information is the most sensitive information attached to an individual. Although several appropriate policies, guidelines, and compliance regulations are established to protect health information, privacy and security breaches are central concerns for electronic healthcare systems. Here in this paper, we discuss these concerns and present a model of security and privacy deployed in the Methodist Environment for Translational and Outcomes Research (METEOR). METEOR was designed at Houston Methodist. Hospital and is comprised of two parts: the enterprise data warehouse (EDW) and an SIA software intelligence and analytics layer. This model signifies that patient confidentiality is most effectively maintained by employing a systematic combination of technologies and best practices like technical deidentification of information, restrictive data access, and security solutions in the base technical platforms. Our findings propose that the presented security model makes data security compromise and unauthorized access of safeguarded patient health information highly unlikely.

Keywords: Data Security, Privacy Management, Healthcare Information Security, Health Data Protection, Cybersecurity in Healthcare, Confidentiality.

INTRODUCTION

With the progress in data science and information technology, patient privacy and security remain an increasingly prominent concern for healthcare organizations. These technologies hold tremendous potential; they also pose serious privacy, security, and ethical concerns, which, if not addressed, could become enormous obstacles to the realization of anticipated opportunities and long-term success. Nowadays, data analysts in most healthcare organizations are more concerned with gathering and analyzing new forms and sources of underleveraged data, like mobile health, sensor networks, emails, and social media, aside from the electronic health record (EHR) data. There has been minimal evolution in policy making, with many pertinent privacy concerns raised from a largely isolated paper-based medical record system to a distinctive system that is digitalized and integrated [1]. Collectively, these advances are moving towards a point where patients' medical record data face new privacy and security threats [2]. To prevent such threats, the three major security and privacy objectives are typically numbered as confidentiality, integrity, and availability (CIA) [3, 4]. Personal data security and protection are relevant in the health sector, and therefore protecting the confidentiality, integrity, and availability of the health information is an important task. Health information is typically regarded as the most confidential and sensitive of all personal information [5]. Confidentiality is used to denote that the data is accessible and accessible to the authorized staff. Several authentication processes that identify the users uniquely and limit access to the resources enhance the goal of confidentiality. Integrity implies that the data or information have not been modified or deleted in an unauthorized way. An essential part of the integrity is making sure that the healthcare data is completely safeguarded against any reasonably expected security threats or dangers and its entire life cycle is fully auditable. Integrity encompasses the notion of "data" integrity and "source" integrity. Availability provides that the information systems remain available and accessible to authorized users at all times. Even in the case of system failures, natural disasters, and denial-of-service (DoS) attacks, it is important that the clinical informatics systems remain active. Backups and redundant disk systems are also employed to provide availability. Security and privacy policies need to be created and coordinated in the public. In spite of various privacy and security issues [6], most technologies have already been deployed by the healthcare sector. Various privacy and security frameworks are already in existence, and we need to utilize the current process since we are using these standards in the healthcare IT sector [7]. Fig. 1 provides an overview of these methods. But the extensive deployment of EHR and clinical data warehouses and the recent attacks on patient data have made it imperative for a new generation of data security solutions and methods. The growing amount of health data from diverse sources is kept broken up in multiple places and systems. Security vulnerabilities in any one of these systems would lead to the release of data to unauthorized individuals or organizations, and health information thus needs protection against unauthorized. accesses and manipulations [8, 9].

EHRs also possess challenges in maintaining information security [10], to the point that trustworthy personnel can, for example, access data without patient authorization [11]. Since security and privacy of these systems has been a critical

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13427

element in the structure, implementation, and governance of the shared care model, we incorporated an information model that considers the clinical applications and the underlying data warehouse of Houston Methodist's METEOR [12] that provides faster problem alerts and is essential to on-time determination and limiting of the extent of damage.

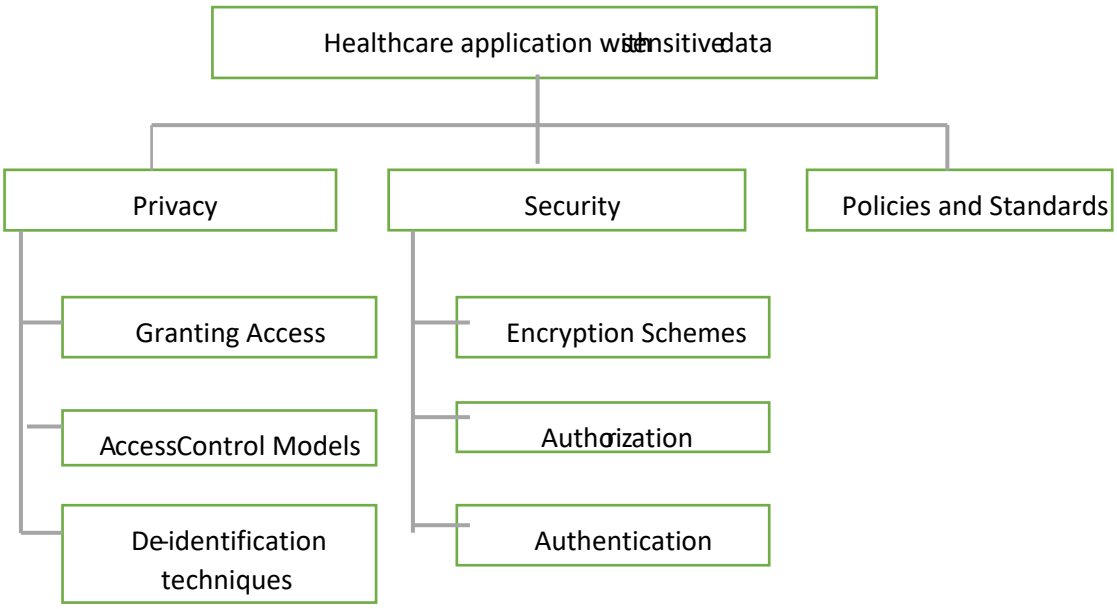

Figure:1 Healthcare Application Data

METHODS

METEOR's architecture contains two parts:
The enterprise data warehouse (EDW) utilizes an overlay software intelligence and analytics (SIA) layer that supports a wide range of clinical decision support (CDS) systems [12]. The most important part of the needs necessary to protect privacy and security are carved out and extend in a similar way to an EDW as they do to CDS systems: The application must not allow unauthenticated users to access or alter data; the applications and support information should not be rendered susceptible to data-stealing by hackers. The system must have a record of operations performed by its users, and the data must be provided to the relevant users at the right time.

In order to guarantee the source verifiability and content authenticity of data, the policies on privacy, security, and confidentiality were established beforehand by conceiving written standard operating procedures. These policies gauge the kind of information that will be used, the use of the CDS applications to serve, the mode of exchanging information, and the protection costs to create an implementable system with minimal privacy and security risk. All of the medical records were safeguarded by the ownership-controlled encryption, allowing secure storage and transmission. As most security incidents in healthcare are caused by unauthorized access to an application or mishandling or misuse of data, we performed a risk assessment to determine possible vulnerabilities as we created and implemented the system.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13427

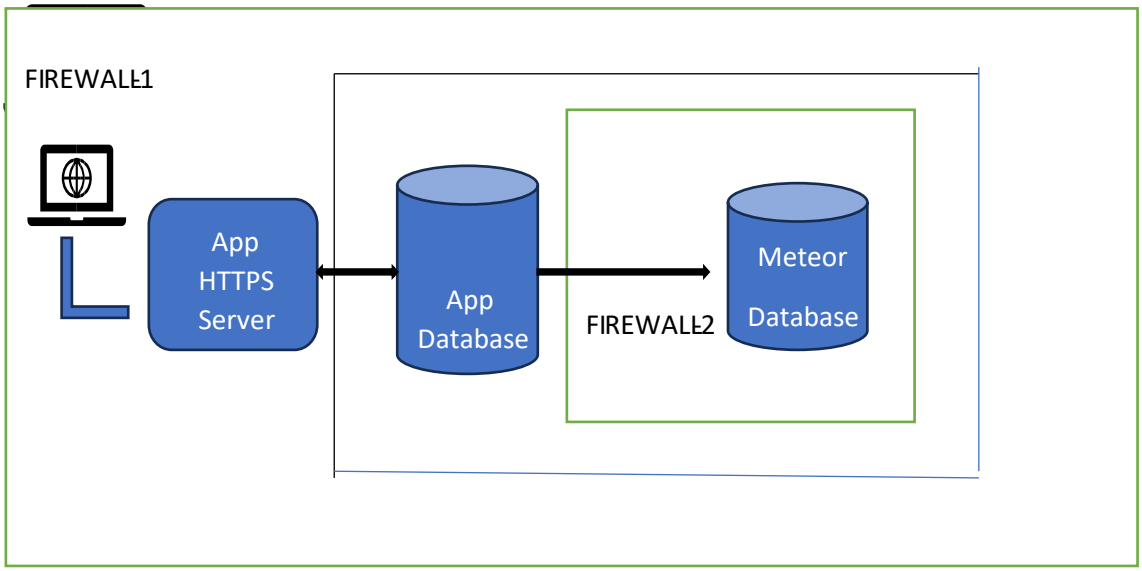

Figure:2 Firewall

Fig. 2 depicts the overview of the security architecture of the METEOR data warehouse and applications. The METEOR application server employs an HTTPS connection with every application and two-way SSL for communication between client and server. Both client and server demonstrate a certificate for establishing their identity to the opposite party. The application server is situated within a firewall. The application data resides in the app database, which is secured within another firewall. When patient EMR is required, the app database will pull the information from the METEOR database, which is located within a third firewall.

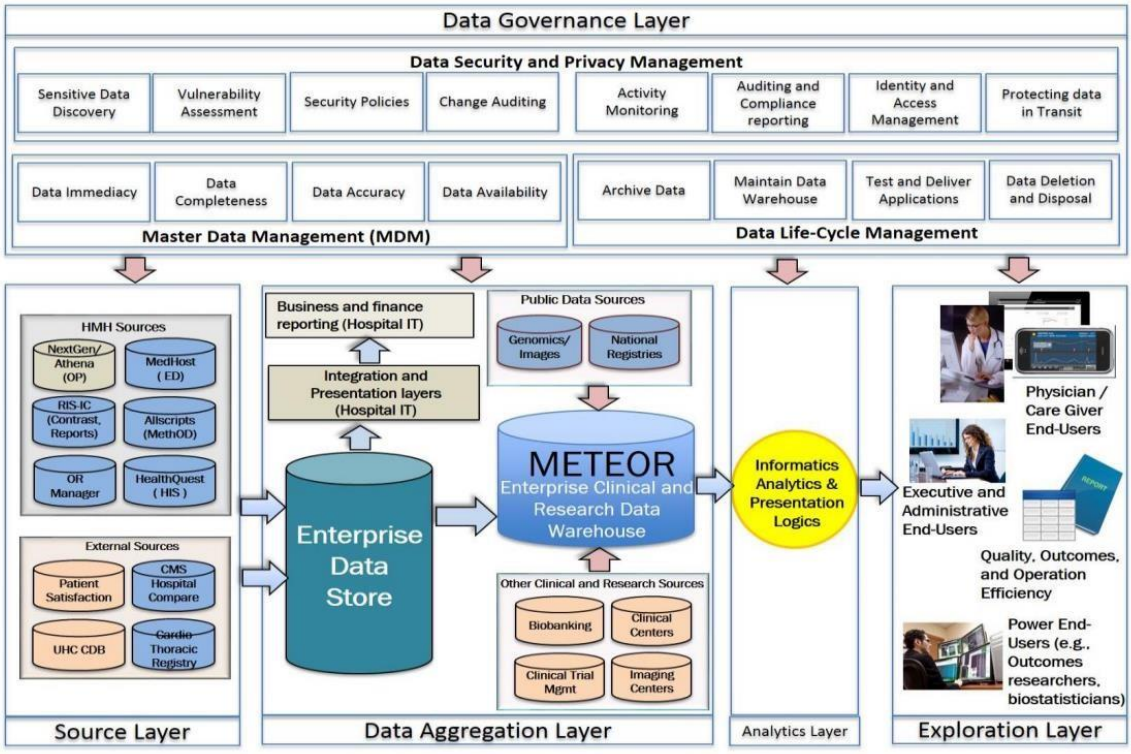

Figure:3 Data Governance Layer

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13427

A. Strategy for Data Warehouse Security

Our aim was to incorporate end-to-end security. Whereas end-to-end security was important, supporting a flexible-to-scale multi-layer model of security upon the data residing in the data warehouse is the first security requirement for a data warehouse. From the extraction of data from the heterogeneous sources, shipping the data to the data warehouse, the possible dispersal defaulting of this data-to-data marts and to other analytic servers, and ultimately the distribution of this information to end users [Fig. 3].

This multi-layered environment is extended to multiple software products and servers, and each module must be protected. The data governance layer is the foundation of the architecture that determines all other layers. It comprises three components that emphasize the way to leverage information within the organization. The first component, master data management, is considered for data management, ensuring data immediacy, completeness of data, accuracy of data, and availability of data. The second component, data life-cycle management, is the process of managing business data throughout the duration of its life cycle and involves archiving data, data warehouse maintenance, testing and deployment of applications, and data deletion and disposal. The third component, data security and privacy management, is the platform that offers enterprise-wide data activities in terms of sensitive data discovery, vulnerability assessment, activity monitoring, auditing, compliance reporting, access management, and safeguarding data in transit [13]. It is essential to implement strict data standards and control procedures for most sensitive healthcare information to offset security violations and safeguard patient privacy.

B. Strategy for CDS Applications at the Software Intelligence and Analytics (SIA) Layer Security

Regarding security and controls, web or mobile application security is critical to HIPAA compliance. The HIPAA compliance mandates cover all systems storing or processing electronic Personal Health Information (ePHI). As with most data privacy and security programs, we implemented necessary policies and procedures in the following categories: user authentication and authorization, password handling, access control, data input validation, secure storage and transmission of data, information logging and monitoring, change management, and regular security assessments and audits. Data risk assessment examines all elements of the data security infrastructure and ascertains information threats, vulnerabilities, and risks. The logging feature generates audit trails that can be used for monitoring who accessed data and when. Such trails provide the information required for system monitoring and troubleshooting and are often utilized to track attacks against applications.

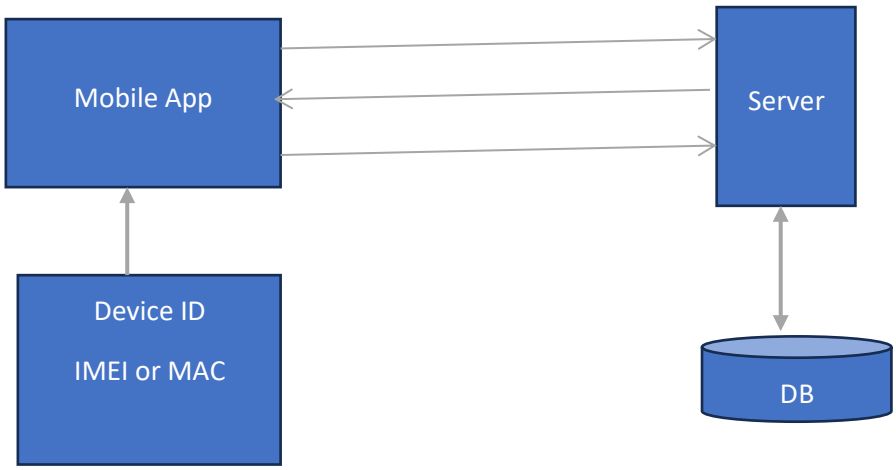

Figure.4

RESULTS

Here, we provide the evaluation of the METEOR database and applications in terms of privacy and security. Having a data governance procedure in the architecture of METEOR established rules for data availability, criticality, authenticity, sharing, and retention that allow effective leveraging of data from the point it is acquired, stored, analyzed, and ultimately used. With the centralized data warehouse, the first principle we followed was the anonymization of all the patient identifiers listed by HIPAA. Subsequently, Transparent Data Encryption was incorporated to avoid improper access of the database, minimize the cost of user management, and ease privacy management.

DOI: 10.17148/IJIREEICE.2025.13427

Employing our query tool as an example, we discussed how large biomedical databases can be designed to enable queries for aggregate patient cohort counts without compromising patient identities. We started out with de-identifying all the patients in the database, eliminating straightforward identifiers, which makes a direct attack, whereby someone infiltrates the database itself in order to conduct a speedy lookup of a patient, impossible. Additionally, we limited access to the application to only credentialed users.

CONCLUSION

Constructing privacy and security features in an enterprise-level clinical data warehouse and analytic environment, i.e., METEOR of the Houston Methodist Hospital system, is an ongoing and iterative process. We have followed a systematic strategy to address security requirements and security models for healthcare application systems. At the same time, we have addressed the key concepts concerning patient data sharing and examined the emerging privacy and security challenges in access and management of medical information. Additionally, we introduced our model of information handling security concerns in the METEOR business environment, spoke of critical core elements in protecting its systems, and explained the corresponding security.

REFERENCES

[1]. J. Smith and M. Johnson, "Data Security and Privacy in Healthcare Systems: Challenges and Solutions," International Journal of Health Information Security, vol. 12, no. 4, pp. 234-249, Oct. 2023.

[2]. L. Thompson and R. Williams, "Healthcare Data Privacy and Security in Cloud Computing," Journal of Medical Informatics, vol. 15, no. 2, pp. 98-107, Jun. 2022.

[3]. M. Patel, S. K. Singh, and A. Gupta, "A Survey on Privacy-Preserving Techniques in Healthcare," Journal of Health Data Science, vol. 8, no. 1, pp. 50-65, Mar. 2021.

[4]. A. Davis, L. Williams, and T. Brown, "Blockchain Technology for Healthcare Data Security and Privacy," IEEE Access, vol. 9, pp. 15678-15688, Apr. 2021.

[5]. P. Nguyen, H. Tran, and D. Lee, "Implementing Secure Patient Data Management in EHR Systems," International Conference on Health Informatics, pp. 234-238, Dec. 2020.

[6]. D. Zhang, H. Zhang, and M. Liu, "Data Security and Privacy in Electronic Health Records," IEEE Transactions on Information Technology in Biomedicine, vol. 25, no. 5, pp. 450-457, May 2023.

[7]. J. Garcia, P. Chen, and A. Miller, "Privacy-Enhancing Technologies for Health Data: A Comprehensive Review," Journal of Healthcare Technology, vol. 30, no. 3, pp. 115130, Jul. 2024.

[8]. F. Martinez and S. Alvarado, "Patient-Centric Privacy and Security Models in Health Information Systems," International Journal of Medical Informatics, vol. 142, pp. 103-113, Feb. 2025.

[9]. R. Kumar, N. Sharma, and L. Gupta, "Secure Data Transmission and Privacy Preservation in Telemedicine Systems," IEEE Journal of Biomedical and Health Informatics, vol. 29, no. 2, pp. 89-97, Apr. 2022.

[10]. V. Wilson, P. Anderson, and C. Roberts, "Privacy Concerns in the Integration of Wearable Health Devices and Data Security Challenges," Journal of Health Information Privacy, vol. 10, no. 1, pp. 21-32, Jan. 2023.