International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 05, ISSN No. 2455-2143, Pages 26-30
Published Online September 2023 in IJEAST (http://www.ijeast.com)

THROUGH THE LENS OF PRINCIPLED DATA PRACTICE A GROUNDBREAKING EXPLORATION INTO ETHICAL HEALTHCARE PLATFORMS

Narayan Hampiholi
Department of AI & Data, AM&C
Distinguished Engineer
Deloitte Consulting LLP, Minneapolis, MN, USA

Abstract - **Fundamental Ethical Principles of Data Privacy and Security and how Healthcare Data Platforms Ensure the Confidentiality and Integrity of Patient Information, Safeguarding it Against Unauthorized Access and Cyber Threats. In the last years, there has been a considerable increase in the usage of electronic health records (EHRs). Credit card numbers, full name, bank account numbers, social security numbers, street addresses, phone numbers, passport numbers, treatments, and medical histories are all private patient information that may be found in health information systems. This information must be safeguarded against manipulation and fraud by other parties. EHRs are anticipated to boost healthcare delivery effectiveness, enhance the standard of care, and reduce mounting budgetary strain. Despite these advantages, there is a possibility that security issues with EHRs compromise patient data confidentiality and privacy. This research paper focuses on the ethical principles—privacy, ownership, transparency, data security, informed consent, data minimization, purpose limitation, and accountability—to help guarantee that patient databases maintain the confidentiality and integrity of patient information while protecting it from unapproved access and online threats. Additionally, numerous systems for privacy and integrity, such as vulnerability analyses and role-based access control, support the objectives of contemporary healthcare while preserving patient privacy.**

Keywords—**AI, Machine learning, Healthcare Data Platform, Data security, GDPR, HIPA**

I. INTRODUCTION

The healthcare sector has changed digitally due to smart devices, the Internet of Medical Things, cloud services, and information systems. Digital medical amenities have allowed more people to receive treatment, which has dramatically improved the quality of life. However, external, and internal threats have made the modern healthcare sector the principal victim. Data breaches harm stakeholders, enterprises, clients, and organizations and are a worry and challenge for security specialists. Despite the variety of data breaches, they virtually always have a comparable effect [1]. Most healthcare records face threats from IT/hacking. Besides, these data face unauthorized disclosures.

One primary source of healthcare digital records is the electronic health record (EHR). EHR has replaced paper-based procedures in the medical sector, enabling it to provide its clients with improved and less expensive services. This has been made possible by advancements in communication and information technology. EHRs promote patient care, encourage patient participation, increase practice effectiveness, aid in illness diagnosis, and render patient medical data always available [1,2]. Healthcare data has grown more electronic, dispersed, and portable during the past few years. In this regard, the Internet of Medical Things (IOMT) has also been essential. Medical enterprises acquire confidential information from their clients and keep it saved on network servers so that it is always available and may be used to improve patient care.

However, as mentioned, a significant source of data privacy violation is the usage of smart gadgets like smartphones or computers. Information databases are occasionally exposed to unauthorized individuals due to human errors, software flaws, and security lapses [1, 3]. As a result, sensitive data is exposed through data breaches. Sensitive healthcare data may occasionally be lost, stolen, or disclosed due to insider attacks that harm protected health information [1].

A comprehensive data file for a single individual might cost hundreds of dollars. Compared to other data organizations, the healthcare sector is among the most negatively impacted.

For instance, a report by Steve Alder from the Health Insurance Portability and Accountability Act (HIPAA) indicates that 'there were 38 healthcare data breaches of 500 or more records reported to the Department of Health and Human Services' Office for Civil Rights in December 2019, an increase of 8.57% from November 2019' [4].

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 05, ISSN No. 2455-2143, Pages 26-30
Published Online September 2023 in IJEAST (http://www.ijeast.com)

Figure 1 below indicates that as from 2014 to 2019 there were over 207,731,022 healthcare records breached.

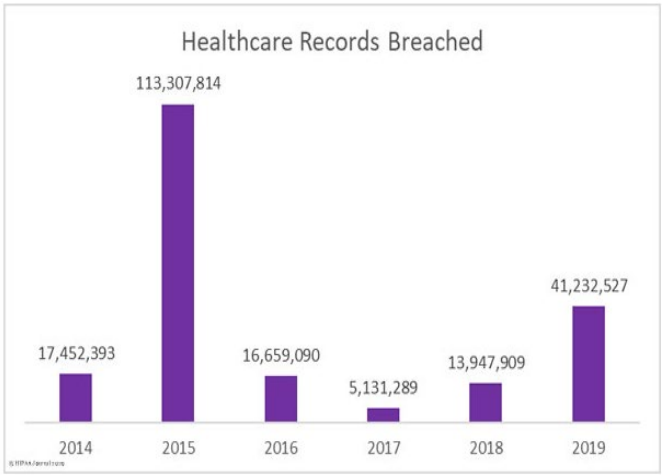

Fig. 1. Healthcare records breached as from 2014 to 2019 [4].

Based on this report, this research paper dives deeply into the core moral precepts governing data privacy and security. It examines how healthcare data platforms protect patient information from unauthorized access and online threats while preserving confidentiality and integrity.

Fundamental Ethical Principles of Data Privacy and Security

In the current digital world, data privacy and security are crucial factors controlled by several basic ethical standards. These guidelines give individuals and organizations a framework for handling data ethically and defending the rights and interests of data subjects. Fundamental ethical principles of data privacy and security are the guidelines that ensure people's data are used appropriately and that their privacy and data are well protected.

There are several ethical principles that healthcare organizations should consider when handling patients' data, including privacy, transparency, ownership, data security, consent, data minimization, purpose limitation, accountability, data accuracy, data retention, and non-discrimination.

Privacy

When healthcare providers handle patients' data, they should ensure the subjects' privacy. Data and information can be collected from patients who are admitted to a hospital or want outpatient treatment. These personal identifiable information (PII) are linked to patients' identity, including credit card number, full name, bank account number, social security number, street address, phone number, and passport number [5]. Privacy protection for people is crucial. Individuals have the right to determine how their personal information is gathered, utilized, and shared, which is their right to privacy. Informed permission, restricting data collection to what is required, and allowing people to view and correct their data are all ethical practices.

Transparency

Healthcare organizations must be open and honest about how they handle data. This entails being transparent about data collection, processing, and usage. Transparency fosters trust and enables people to choose wisely when sharing their data. It is dishonest, illegal, and unjust to the data subjects when an organization withholds information or lies about its procedures for collecting data and its purposes for using it [5].

Ownership

A crucial ethical principle of data privacy and security is ownership. At all points, individuals are the owners of their data. Collecting patients' personal information without their knowledge is illegal, unacceptable, and considered theft. Healthcare organizations should ask their clients whenever they want to use their data and ensure that this data usage is within the acceptable rules and regulations of data usage.

Data Security

This is among the major ethical principles on which this research paper is based. Healthcare organizations should ensure their data is safely secured, whether stored in the Cloud, hard disk or drive. Security should focus on preventing data theft, breaches, and unauthorized access by both internal and external parties.

Consent

Before collecting and processing patient data, every healthcare organization should get the patients' informed and voluntary consent. Consent must be easy to revoke, explicit, and precise [6]. People ought to have the option to refuse data gathering. The written declaration of consent needs to be prepared in plain language that individuals can understand; it needs to reduce the chance of undue or coercion influence, and the subject needs to be given enough time to think about participating in the data collection [6].

Data Minimization

Organizations should collect only the information required to get the desired results. Avert gathering too much or unrelated data. Data reduction lowers the chance of abuse and data intrusions [7].

Purpose Limitation

Only the intended application of the data should be made of it. Healthcare entities should only utilize data for new purposes if they have permission or a valid legal justification [8].

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 05, ISSN No. 2455-2143, Pages 26-30
Published Online September 2023 in IJEAST (http://www.ijeast.com)

Accountability
Healthcare organizations are responsible for their data handling procedures. This entails putting in place explicit policies and processes, designating a Data Protection Officer (DPO) if needed, and being ready to provide evidence that data protection legislation and rules have been complied with [8]. It is essential to emphasize that following these core ethics.
Data privacy and security principles are significant to earning patients' confidence, ensuring conformity to rules and laws, and reducing potential risks in managing data in the digital era.

Ensuring Confidentiality and Integrity of Patient Information, Safeguarding It against Unauthorized Access and Cyber Threats
Several threats undermine crucial data in healthcare, banking, and related industries in the modern era. There have been data breaches since the introduction of electronic health records, a significant breakthrough in keeping patient data, advancing medical research, digitalizing medical procedures, and improving administrative efficiency. The integrity and confidentiality of patient information are the main problems this digital transition has brought about.
Maintaining patient privacy, believing in healthcare organizations, and complying with strict regulatory standards depend on healthcare data security. Healthcare data platforms are tasked with crucial concerns of confidentiality and integrity in ensuring that unauthorized individuals and cyber threats do not access vital patient data. These platforms apply various mechanisms and technologies to help mitigate these privacy issues.

Confidentiality Mechanisms and Technologies in Safeguarding Patient Data
Confidentiality within the healthcare sector ensures that all patient information is kept private and only accessed by authorized personnel within the organization. The various mechanisms and technologies that healthcare data platforms can apply in maintaining patient data include data encryption, access control mechanisms, and secure user authentication.

1. Data Encryption
Data encryption is a proven method of limiting unauthorized access to patients' critical data. It provides security at every data stage, from the data storage center to the endpoint. This means that when administrators, physicians, and clinicians access data on their computers, smartphones, or tablets, it is safe from outside intrusion [9]. Encryption is crucial in protecting data against breaches like storage device theft and packet sniffing. The encryption method must be adequate, user-friendly for workers and patients, and easily expandable to accommodate additional electronic health data.
It is also best to limit the number of keys each party holds. Various encryption algorithms can be devised and implemented quite well. The Rijndael and Blowfish are the most applied encryption algorithm that is efficient, secure, flexible, and easy to implement [10].
Two types exist among the data encryption algorithms: Data-at-Rest Encryption and Data-at-Transit Encryption. Data-at-Rest Encryption is applied to safeguard data on databases, servers, and related storage devices. This type of encryption protects against external data intrusion. Besides, Data-at-Transit Encryption enables data to be encrypted during transmission between computers using the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocols, preventing unauthorized parties from intercepting it [9].

2. Access Control Mechanisms
Access Control Mechanisms are grouped into Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC). The process of proving or confirming that statements made concerning or regarding a topic are truthful and legitimate is known as authentication. Authentication performs essential tasks for every company, including preserving user identities, safeguarding access to organizational networks, and verifying that the user in question is who they claim to be[9]. In the case of healthcare databases, by requesting several kinds of identification, including a password and a fingerprint, from users before granting access to patient data, authentication offers an additional layer of protection in the context of MFA. Only individuals with authorized access are allowed by the system to access or retrieve patient data. Besides, authentication can help prevent man-in-the-middle (MITM) attacks by incorporating TLS and SSL protocols. These protocols ensure that end-to-end network connection at the transport layer is encrypted [9]. When users enter a healthcare system, their identities, and the healthcare information they submit should be validated.
Furthermore, Role-Based Access Control (RBAC) is another crucial way of ensuring confidentiality and integrity of patient information, safeguarding it against unauthorized access. RBAC limits network access per the individual's role in the organization. Only the information needed for employees to do their jobs efficiently is given to them. Access may depend on several variables, including authority, responsibility, and job ability [11].
The capacity to read, create, or alter files is only one example of how access to computer resources might be restricted to particular activities. It is crucial to note that only employees with higher clearance access should be allowed to access or modify patients' data in any healthcare database.

3. Secure User Authentication
Secure user authentication keeps strangers from accessing patients' sensitive information. If user authentication is unsafe, cybercriminals may be able to gain entry to a system and obtain data. The most common secure user authentication includes password-based authentication, certificate-based authentication, and biometric authentication. Patients entering

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 05, ISSN No. 2455-2143, Pages 26-30
Published Online September 2023 in IJEAST (http://www.ijeast.com)

their data online should be prompted to enter a more secure password with letters, numbers, and special characters. This is also crucial for these databases, and they should choose different passwords for their various databases. Also, certificate-based authentication allows a user computer to identify itself to a server computer using a special public-key certificate; these key certificates are unique to users.

A modern approach to safeguarding patient data is through biometric authentication. The most common biometric authentications include facial recognition, speaker recognition, eye scanners, and fingerprint scanners [14]. These authentications rely on a person's distinctive biological traits. Biometric authentication can be used with other security protocols like password authentications and multi-factor authentication, adding a layer of security. In ensuring the data confidentiality of patients, healthcare platforms can apply these security mechanisms and techniques and inform their patients to do the same.

Integrity in Healthcare Data Platforms

As long as patient data are secure and confidential, there is a dire need to maintain the integrity of these healthcare data platforms to ensure patient information consistency, reliability, and accuracy. Data integrity prevents unauthorized changes, corruption, or manipulation of patient information [13]. This can be achieved through data validation and verification, disaster and backup recovery, data auditing, threat detection and prevention, incident response plans, and vulnerability assessments.

Data Validation and Verification

Healthcare data platforms should use data validation criteria like content, format, and relationship to ensure the information input in various electronic health records is accurate and complete. Some common data types that can be validated and verified within the EHRs include laboratory results, demographics, medications, patient identifiers, vital signs, procedures, and diagnoses [12]. This can help in flagging errors for correction or various inconsistencies. Digital signatures may be utilized to verify the origin of data modifications, guaranteeing that only persons with the proper authorization may update patient information, thus improving data integrity.

Disaster and Backup Recovery

Data integrity relies on the consistency, reliability, and accuracy of data, and healthcare data platforms can ensure that data remains reliable and accurate by providing automated frequent information backups [13]. Cloud-based backups can help prevent crucial data from getting lost due to hardware failures, natural disasters, or cyberattacks. Cloud-based technologies are inherently secure. With the aid of digital signatures, unique keys, and two-factor authentication, they also offer encryption and protection options when used as a component within a medical system. Besides, it is also crucial to provide off-site storage for patients' data; this ensures that data are safe even in the pretext of catastrophic incidences.

Data Auditing

The integrity of healthcare data platforms should be based on data auditing. Several tools can be used to monitor and detect anomalies, data changes, or suspicious activities that can lead to hacking or related illegal activities [15]. These data auditing tools, like Cisco Stealth watch and Flow Mon NBAD, offer real-time alerts, extensive network behavior awareness, and continuous network surveillance. Also, Regular data validation checks support maintaining data integrity by identifying and resolving conflicts or inconsistencies in patient records.

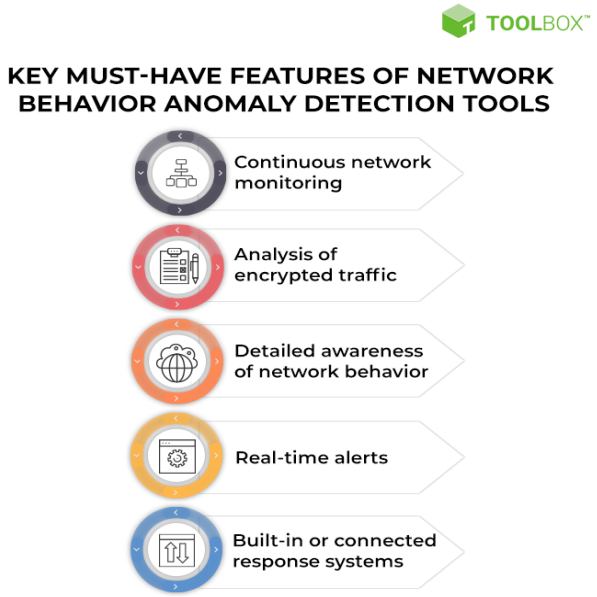

Fig. 2. A breakdown of what anomaly detection can do [15].

Figure 2 depicts what anomaly detection can do including providing real-time alerts, encrypted traffic analysis, continuous network monitoring, and detailed awareness of network behavior [15].

Incident Response Plans

Healthcare data platforms should have an incident response team trained to act quickly during a security breach, limiting harm and safeguarding patient data [16]. Also, to increase their integrity, there should be precise communication mechanisms to ensure that patients, law enforcement, and regulatory agencies are informed in case of any data breach.

Vulnerability Assessments

Regular scanning can prevent major threats before hackers take advantage of security flaws in healthcare data systems. Patching and updating software and systems on schedule assists in fixing known vulnerabilities. Besides, the security of EHR systems and databases may be enhanced by

administrative functions. Such as thorough training, security strategies, and the presence of a chief information security officer [16]. Additionally, administrative features like requiring manager consent before data releases and teaching staff to handle missing data can improve health records database security.

II. CONCLUSION

This research intended to provide actionable recommendations and guidelines for the ethical design, implementation, and operation of healthcare data platforms that foster responsible data management practices upholding patient data security, privacy, and ethical principles. The ethical principles highlighted, including privacy, transparency, ownership, data security, informed consent, data minimization, purpose limitation, and accountability, help ensure that patient databases provide the confidentiality and integrity of patient information, safeguarding it against unauthorized access and cyber threats. Besides, various confidentiality and integrity mechanisms like vulnerability assessments and role-based access control help maintain patient privacy while advancing modern healthcare's goals.

III. REFERENCES

[1]. A.H. Seh et al. 2020, "Healthcare data breaches: Insights and implications," Healthcare, vol. 8, no. 2, p. 133, doi: https://doi.org/10.3390/healthcare8020133 .

[2]. K. Adane, M. Gizachew, and S. Kendie, 2019, "The role of medical data in efficient patient care delivery: A review," Risk Management and Healthcare Policy, vol. Volume 12, no. 12, pp. 67–73, doi: https://doi.org/10.2147/rmhp.s179259

[3]. "Chapter 6 -- Information Security, from Safeguarding Your Technology, NCES Publication 98-297 (National Center for Education Statistics)," nces.ed.gov. https://nces.ed.gov/pubs98/safetech/chapter6.asp

[4]. S. Alder, Jan. 21, 2020, "December 2019 Healthcare Data Breach Report," HIPAA Journalhttps://www.hipaajournal.com/december-2019-healthcare-data-breach-report/

[5]. C.Cote, Mar. 16, 2021, "5 Principles of Data Ethics for Business," Business Insights Blog. https://online.hbs.edu/blog/post/data-ethics#:~:text=Ownership

[6]. S. Manti and A. Licari, May 2018, "How to obtain informed consent for research," Breathe, vol. 14, no. 2, pp. 145–152, doi: https://doi.org/10.1183/20734735.001918 .

[7]. M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, 2020, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1–1, doi: https://doi.org/10.1109/comst.2019.2962586 .

[8]. L. Irwin, Aug. 14, 2019, "The GDPR: Understanding the 6 data protection principles," IT Governance Blog, doi:https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles

[9]. K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, 2018, "Big healthcare data: preserving security and privacy," Journal of Big Data, vol. 5, no. 1, doi: https://doi.org/10.1186/s40537-017-0110-7 .

[10]. "How does the encryption algorithm Rijndael work?," www.password-depot.de. doi:https://www.password-depot.de/en/know-how/blowfish-and-rijndael.htm

[11]. E. Zhang, Nov. 07, 2022, "What is Role-Based Access Control (RBAC)? Examples, Benefits, and More," Digital Guardian. doi: https://www.digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more

[12]. V. Ehrenstein, H. Kharrazi, H. Lehmann, and C. O. Taylor, 2019 “Obtaining Data From Electronic Health Records”. Agency for Healthcare Research and Quality (US). Available: doi:https://www.ncbi.nlm.nih.gov/books/NBK551878/

[13]. "Data Integrity vs Data Quality: Nah, They Aren't Same!," atlan.com, Aug. 04, 2023. https://atlan.com/data-integrity-vs-data-quality/#:~:text=Data%20integrity%20refers%20to%20the%20accuracy%2C%20consistency%2C%20and%20reliability%20of.

[14]. G. D. Maayan, "5 User Authentication Methods that Can Prevent the Next Breach," ID R&D, Feb. 07, 2020. doi: https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/#:~:text=User%20authentication%20is%20a%20method

[15]. C.BasuMallick, "Top 10 Network Behavior Anomaly Detection Tools in 2022," Spiceworks, Mar. 08, 2018.doi: https://www.spiceworks.com/tech/networking/articles/network-behavior-anomaly-detection-tools/

[16]. N. N. Basil, S. Ambe, C. Ekhator, and E. Fonkem, 10, Oct. 2022, "Health Records Database and Inherent Security Concerns: A Review of the Literature," Cureus, vol. 14, no, doi: https://doi.org/10.7759/cureus.30168 .