Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 203 (2025) 1-39 EISSN 2392-2192

A Systematic Review of Security, Privacy, and Compliance Challenges in Electronic Health Records: Current Practices and Future Directions

Damilola Osamika[1], Bamidele Samuel Adelusi[2], Maria Theresa Chinyeaka Kelvin-Agwu[3], Ashiata Yetunde Mustapha[4], Adelaide Yeboah Forkuo[5], Nura Ikhalea[6]

[1]Independent Researcher, Ohio, USA

osamikadamilola@yahoo.com

[2]DevOps Engineer/Cloud Solutions Architect, Swoom, USA

deleadelusi@yahoo.com

[3]Independent Researcher, Bolton, Greater Manchester, UK

realmaria.kelvin@gmail.com

[4]Kwara State Ministry of Health, Nigeria

mustaphaashiata@gmail.com

[5]Independent Researcher, USA

ayeboahforkuo@gmail.com

[6]Independent Researcher, Texas, USA

Nuraaniya@gmail.com

Corresponding Author: osamikadamilola@yahoo.com

(Received 10 February 2025; Accepted 22 March 2025; Date of Publication 6 May 2025)

ABSTRACT

Electronic Health Records (EHRs) have transformed modern healthcare by enabling efficient data storage, access, and sharing across providers and institutions. However, the rapid digitization of sensitive patient information has introduced significant security, privacy, and compliance challenges that threaten patient trust, data integrity, and regulatory adherence. This systematic review critically examines current practices, emerging threats, and future directions concerning the protection of EHRs within healthcare systems. A comprehensive literature search was conducted across major databases, including PubMed, IEEE Xplore, Scopus, and ScienceDirect, targeting peer-reviewed articles published between 2015 and 2024. A total of 86 relevant studies were selected and analyzed based on inclusion criteria focused on EHR security frameworks, privacy-preserving techniques, legal compliance (e.g., HIPAA, GDPR), and case studies of healthcare data breaches. The review categorizes challenges into technical, organizational, and regulatory domains and evaluates the effectiveness of various mitigation strategies. Findings reveal that while encryption, access control, and anonymization are widely adopted technical safeguards, many implementations remain vulnerable to insider threats, misconfigurations, and inadequate monitoring. Privacy concerns are further amplified by third-party integrations and the growing use of mobile health applications, which often fall outside traditional compliance oversight. From a regulatory perspective, inconsistencies in global standards and the complexity of compliance obligations hinder seamless adoption and enforcement. Emerging solutions, including blockchain, federated learning, and differential privacy, show promise in enhancing security and privacy without compromising data utility. However, their scalability and integration into legacy systems remain ongoing challenges. The review highlights the need for harmonized regulatory frameworks, continuous staff training, real-time monitoring, and multidisciplinary collaboration to address evolving cybersecurity threats. This study provides a comprehensive synthesis of the state of EHR security, offering valuable insights for healthcare providers, policymakers, and technology developers. It emphasizes the urgency of proactive strategies to safeguard digital health infrastructures while fostering innovation and patient-centered care.

Keywords: Electronic Health Records, EHR Security, Data Privacy, HIPAA Compliance, Cybersecurity, Healthcare Technology, Patient Data Protection, Systematic Review, Blockchain, Privacy-Preserving Technologies.

1. INTRODUCTION

Electronic Health Records (EHRs) have fundamentally transformed patient information management in healthcare settings. Their digital nature has facilitated the transition from traditional paper-based systems, resulting in enhanced efficiency of clinical workflows and improved coordination among healthcare providers. This transition not only streamlines operations but also significantly improves patient care outcomes by allowing for real-time access to critical health information such as medical histories, test results, and treatment plans (Rezaeibagha et al., 2015; Adeniyi et al., 2024). Research indicates that while EHR implementation may initially lead to decreased productivity, long-term benefits emerge in terms of improved efficiency and care quality. For instance, a qualitative study found that although EHRs may temporarily reduce productivity, they can lead to significant productivity increases when coupled with performance incentives, such as pay-for-performance programs (Provenzano et al., 2024).

Despite their advantages, the integration of EHR systems into healthcare delivery poses substantial challenges, particularly regarding data security and compliance with regulatory frameworks. The sensitivity of health records, which contain personally identifiable information (PII) and significant medical data, makes them attractive targets for cyberattacks (Adepoju et al., 2022, Gbadegesin et al., 2022). This has been a growing concern, with escalating incidents of data breaches leading to identity theft and financial fraud (Adelodun & Anyanwu, 2024, Chigboh, Zouo, & Olamijuwon, 2024, Ogugua et al., 2024).

Recent literature highlights that around 50% of studies emphasize the importance of security and privacy in EHR systems due to their vulnerability to cyber threats (Kruse et al., 2016). Institutions are tasked with not only protecting this sensitive information but also ensuring compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), which impose stringent requirements on data management practices (Otieno & Loice, 2019; Hoffman, 2016).

Healthcare organizations have faced increasing scrutiny from regulators due to rising cyberattacks and breaches in patient data security, which can result in severe penalties and reputational damage. High-profile incidents underline the urgency for these organizations to bolster their cybersecurity measures while adapting to evolving legal and ethical standards that govern patient data protection (Hackl et al., 2011; Tertulino et al., 2024). As the utilization of technologies such as cloud computing and telemedicine expands, new vulnerabilities necessitate innovative security solutions to safeguard patient data (Oluwole et al., 2023).

This systematic review of existing research aims to scrutinize the multifaceted challenges and solutions related to privacy, security, and compliance in EHR systems. It emphasizes the importance of developing comprehensive strategies to mitigate risks associated with EHR data management while ensuring that stakeholders, including policymakers and healthcare practitioners, are equipped with best practices for securing sensitive patient information (Al-Zubaidie et al., 2019; Tertulino et al., 2023).

2. METHODOLOGY

This study adopted a systematic review approach in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines to investigate the current practices, challenges, and future directions regarding security, privacy, and compliance in Electronic Health Records (EHRs). The literature search was conducted across peer-reviewed journals and digital repositories, focusing on studies published from 2011 to 2025. Keywords such as “electronic health records,” “security,” “privacy,” “compliance,” “cybersecurity,” “HIPAA,” “data protection,” “patient safety,” and “healthcare regulations” were used in various Boolean combinations to retrieve relevant studies.

A total of 220 records were initially identified. Following the removal of 12 duplicate records, 208 articles were screened based on titles and abstracts. 106 articles were excluded for not meeting the inclusion criteria. The full texts of 102 articles were assessed, with 58 articles excluded due to lack of relevance to the core themes of security, privacy, and compliance within EHR contexts or insufficient methodological rigor. Ultimately, 44 studies were included for qualitative synthesis. These studies were assessed for methodological quality, relevance, and thematic contributions using a structured data extraction form. Inclusion criteria comprised empirical, conceptual, and review papers that addressed one or more of the core focus areas within EHR systems. Exclusion criteria included studies that focused solely on EHR usability, digitization logistics, or unrelated healthcare technologies.

The studies selected provided insights into regulatory frameworks, risk mitigation strategies, blockchain and AI integration for EHR protection, cross-jurisdictional compliance mechanisms, and the implications of emerging technologies. Data were synthesized thematically using narrative techniques to identify prevailing concerns, recurring methodologies, and future research needs. The findings were categorized into challenges, current mitigation practices, and forward-looking strategies, guided by both healthcare informatics theory and regulatory frameworks.

The flow of study identification, screening, eligibility, and inclusion is illustrated in the PRISMA flowchart provided in figure 1.

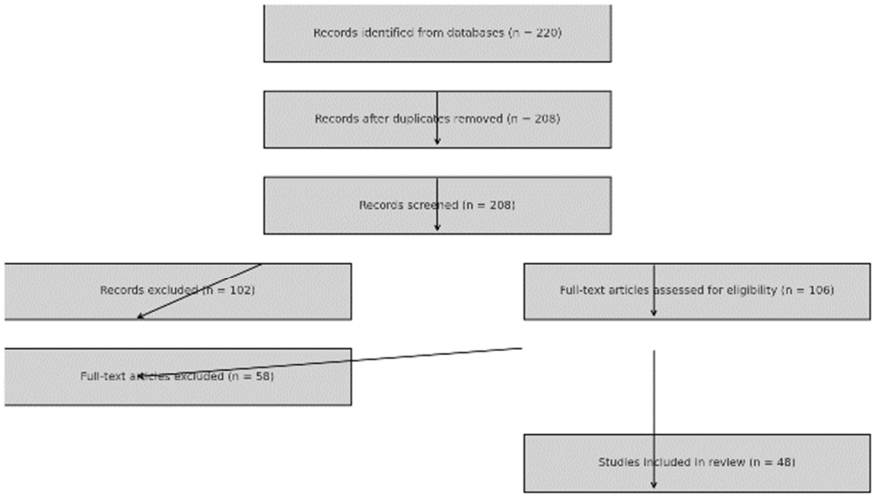

Figure 1. PRISMA flowchart of the study methodology.

3. SECURITY CHALLENGES IN EHR SYSTEMS

Electronic Health Records (EHRs) have transformed the way healthcare providers manage patient information, offering improved accessibility, streamlined workflows, and enhanced coordination of care. However, the widespread digitization of sensitive health data has also introduced a broad array of security challenges that threaten the confidentiality, integrity, and availability of electronic health information (Ayo-Farai et al.. 2024, Chintoh et al., 2024, Odionu et al., 2024). As EHR systems become more complex and interconnected with various healthcare technologies and platforms, they face increasing exposure to security vulnerabilities that must be systematically addressed to ensure patient safety and regulatory compliance.

One of the most significant security challenges facing EHR systems today is the presence of technical vulnerabilities that can be exploited by malicious actors. Unauthorized access remains a primary concern, as attackers often target weak points in system architecture to gain entry to patient records without proper authorization. These breaches may result from poorly configured servers, unpatched software, or insecure network protocols (Adhikari et al., 2024, Chukwurah et al., 2024, Zouo & Olamijuwon, 2024). In many cases, attackers leverage common tactics such as phishing, brute force attacks, or exploiting known software flaws to penetrate systems and extract sensitive data. The impact of such intrusions is severe, as health records contain a rich source of personally identifiable information (PII), including social security numbers, addresses, insurance details, and full medical histories. Figure 2 show Figure of security risks in traditional cloud-based Electronic Medical Record Management Systems presented by Rahman et al., 2019.

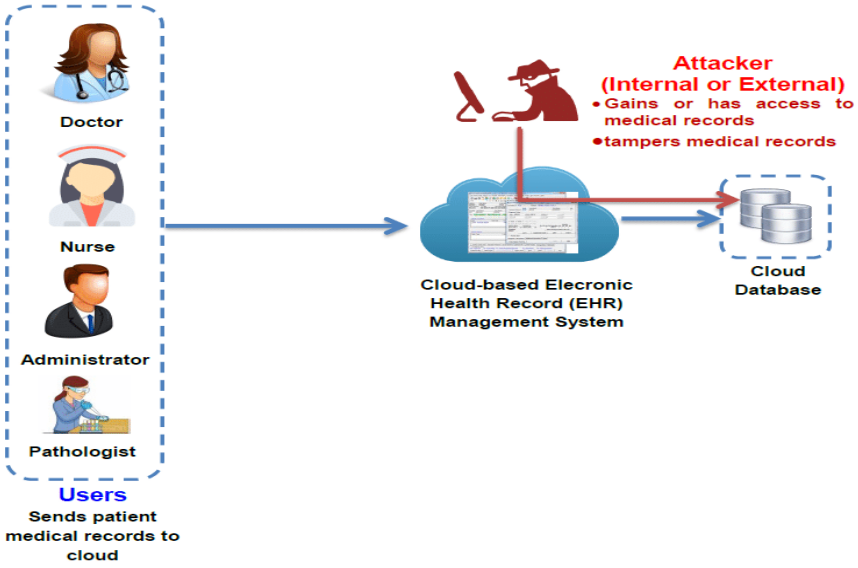

Figure 2. Security Risks in Traditional Cloud-based Electronic Medical Record Management Systems (Rahman, et al., 2019).

Data breaches and malware attacks have become alarmingly frequent in healthcare settings, highlighting the vulnerabilities inherent in current EHR infrastructures. Ransomware, in particular, has emerged as a potent threat, with several high-profile attacks paralyzing hospital operations and compromising millions of patient records. In these incidents, attackers encrypt critical data and demand ransom payments to restore access, often resulting in significant financial and operational damage to healthcare organizations. Malware can also be introduced via infected email attachments, compromised websites, or removable media, spreading across networks and disrupting EHR functionality (Adewuyi et al., 2024, Edoh et al., 2024, Ogunboye et al., 2024). Once inside the system, malicious software can remain undetected for extended periods, collecting data, monitoring user activity, or providing backdoor access to external actors.

Weak authentication mechanisms further exacerbate the risk of unauthorized access and data compromise. Many EHR systems continue to rely on single-factor authentication methods, such as basic username and password combinations, which are highly susceptible to theft or brute-force guessing. Inadequate password policies, lack of multifactor authentication (MFA), and insufficient user session controls increase the likelihood of account compromise, especially when combined with users' poor cybersecurity hygiene (Azubuike et al., 2024, Chigboh, Zouo & Olamijuwon, 2024). In some cases, shared login credentials among healthcare staff or the failure to terminate inactive sessions can inadvertently grant access to unauthorized individuals. Strengthening authentication protocols, including the implementation of biometric verification or time-based one-time passwords (TOTPs), is critical to reducing the attack surface and enhancing system security.

Beyond external threats, insider threats represent another persistent and often underappreciated challenge in EHR security. These threats stem from individuals within the organization who have legitimate access to health records but misuse their privileges—either intentionally or unintentionally. Role-based access controls (RBAC), while designed to limit data access to only what is necessary for specific job functions, are frequently misconfigured or overly broad in practice (Atandero et al., 2024, Chintoh et al., 2024, Ohalete et al., 2024).

This allows users, including administrative staff, nurses, or even custodial personnel, to access more patient information than their roles require. In some cases, employees have been found to access the records of celebrities, acquaintances, or former partners out of curiosity or malicious intent, violating patient privacy and breaching ethical standards. Sharma et al., 2022, presented ethical issues in electronic medical records, shown in figure 3.

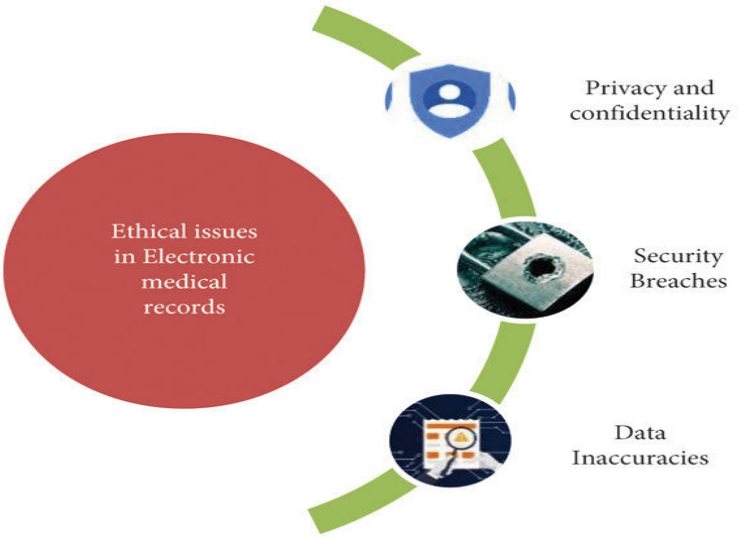

Figure 3. Ethical issues in electronic medical records (Sharma, et al., 2022).

Human error and lack of proper cybersecurity training further amplify the risks associated with insider threats. Even well-intentioned employees may inadvertently compromise EHR security by clicking on phishing links, using weak passwords, or mishandling portable devices containing patient data. The fast-paced and high-stress nature of healthcare environments often contributes to lapses in judgment or attention to detail (Jahun et al., 2021, Matthew et al., 2021). Without comprehensive training and ongoing awareness programs, staff may fail to recognize security threats or follow established protocols, leaving systems vulnerable to exploitation. Encouraging a culture of cybersecurity, backed by regular training sessions and incident response simulations, is essential for reducing the likelihood of internal security failures.

Another critical area of concern lies in the underlying infrastructure and integration components that support EHR systems. As healthcare organizations increasingly rely on third-party applications, mobile health (mHealth) apps, and cloud services, the attack surface for potential breaches has expanded considerably. Third-party integrations can introduce new vulnerabilities, especially when vendors do not adhere to stringent security practices or when APIs (application programming interfaces) are inadequately secured (Adepoju et al., 2024, Folorunso et al., 2024, Olamijuwon & Zouo, 2024). For example, health apps that synchronize with EHRs to track patient fitness or medication adherence may lack end-to-end encryption or transmit data over insecure channels, exposing sensitive information to interception or unauthorized access.

Mobile health applications, while enhancing patient engagement and access to care, present unique security risks due to their deployment on personal devices that may not meet enterprise-grade security standards. Loss or theft of smartphones, lack of device encryption, and weak app permissions management can all result in unauthorized disclosure of EHR data.

Furthermore, poorly designed apps may allow data leakage, store information in insecure locations, or fail to properly authenticate users (Abieba, Alozie & Ajayi, 2025, Chintoh et al., 2025, Oso et al., 2025). Ensuring that all third-party applications undergo rigorous security vetting, are subject to regular audits, and comply with industry standards such as HIPAA and NIST guidelines is imperative for maintaining a secure EHR ecosystem. Electronic health record (EHR) model presented by Boumezbeur & Zarour, 2022, is shown in figure 4.

Figure 4. Electronic health record (EHR) model (Boumezbeur & Zarour, 2022).

Legacy system limitations pose another significant challenge to EHR security. Many healthcare organizations continue to operate on outdated hardware or software platforms that lack support for modern security features. These legacy systems are often incompatible with newer technologies or updates, making them difficult to patch or secure effectively. They may also lack robust encryption, logging, or access control capabilities, leaving them highly vulnerable to intrusion (Ayo-Farai et al., 2023, Babarinde et al., 2023). Migrating to more secure and scalable platforms is often hampered by budget constraints, operational disruption concerns, and the complexity of data migration. However, continuing to rely on antiquated systems not only undermines security but also impedes the integration of innovative technologies needed to improve care delivery and data protection.

The convergence of these security challenges underscores the complexity of safeguarding EHR systems in today's healthcare environment. Technical vulnerabilities, such as unauthorized access, malware, and inadequate authentication, must be addressed through rigorous system hardening, continuous monitoring, and the adoption of advanced cybersecurity tools. Simultaneously, mitigating insider threats requires a strong governance framework that includes role-based access policies, routine audits, and a culture of accountability and awareness (Adhikari et al., 2024, Edoh et al., 2024, Odionu et al., 2024). Infrastructure-related risks—particularly those associated with third-party integrations, mobile apps, and legacy systems—necessitate a proactive approach to vendor management, application security, and strategic IT investment.

As the healthcare industry continues to digitize and embrace data-driven innovation, the importance of robust EHR security cannot be overstated. Ensuring the confidentiality, integrity, and availability of patient data is not only a regulatory requirement but a moral imperative. Without trust in the security of electronic health records, both clinicians and patients may hesitate to fully engage with digital tools, limiting their potential to improve health outcomes (Ariyibi et al., 2024, Chintoh et al., 2024, Olorunsogo et al., 2024). A comprehensive and evolving approach to EHR security—rooted in collaboration among technologists, clinicians, administrators, and policymakers—is essential to building resilient healthcare systems that can meet the demands of the present while preparing for the challenges of the future.

4. PRIVACY CONCERNS

Privacy concerns are among the most critical issues in the implementation and management of Electronic Health Records (EHRs), especially as healthcare systems increasingly rely on digital infrastructure to store, manage, and exchange sensitive patient information. The transition from paper-based records to electronic platforms has undoubtedly enhanced the efficiency and accessibility of healthcare, but it has also raised substantial questions about how patients' personal health information (PHI) is collected, used, and shared (Adepoju et al., 2022, Ogbeta Mbata & Udemezue, 2022). These concerns are compounded by the growing use of advanced technologies such as artificial intelligence (AI) and the Internet of Things (IoT), which, while offering innovative healthcare solutions, introduce complex privacy risks that demand careful scrutiny and proactive governance.

At the center of many privacy debates is the issue of patient consent and data control. In theory, patients should have the right to determine who can access their health information, how it is used, and for what purposes. Consent management systems are designed to support this autonomy by enabling patients to grant, deny, or withdraw consent in a granular and transparent manner. These systems vary in sophistication, from simple opt-in/opt-out checkboxes to more advanced platforms that allow patients to set access permissions for specific providers, data types, or timeframes (Adigun et al., 2024, Hussain et al., 2024, Ohalete et al., 2024). However, in practice, the implementation of effective consent management remains fragmented and inconsistent. Many healthcare providers still rely on blanket consent forms signed at the time of admission, which do not provide meaningful control or awareness over future data uses, particularly in the context of secondary data usage, such as research or marketing (Oladosu et al., 2021).

Data ownership and portability further complicate the landscape of privacy in EHR systems. The question of who truly owns a patient’s data remains legally and ethically ambiguous in many jurisdictions. While patients are considered the subjects of the data, healthcare providers and institutions often act as custodians, controlling access and infrastructure. This dynamic can lead to power imbalances, where patients may find it difficult to obtain complete copies of their records or transfer their data between providers (Adelodun & Anyanwu, 2024, Folorunso et al., 2024, Oshodi et al., 2024). Lack of interoperability between EHR systems exacerbates this issue, undermining the promise of patient-centered care and data fluidity. In some cases, patients may not even be aware of who has access to their information or how it is being shared across the healthcare ecosystem. Strengthening legal frameworks around data ownership, promoting standards for health data portability, and empowering patients with tools to manage their digital identities are essential steps in restoring trust and privacy in electronic health systems.

Another major area of concern relates to the anonymization and de-identification of health data. As health records are increasingly used for secondary purposes such as biomedical research, public health surveillance, and the development of machine learning models, de-identification techniques are employed to protect patient privacy. These methods aim to remove or obscure personal identifiers—such as names, addresses, dates of birth, and medical record numbers—making it difficult to trace data back to individuals (Ayo-Farai et al.. 2024, Ike et al., 2024, Olorunsogo et al., 2024). Common techniques include pseudonymization, generalization, suppression, and data masking. However, the effectiveness of these methods is subject to significant limitations.

Recent studies have shown that even de-identified health data can be re-identified with high accuracy when cross-referenced with other publicly available datasets. For example, combining de-identified health records with demographic data or social media information may enable attackers or researchers to infer individual identities. This risk is heightened when datasets contain unique or rare health conditions, treatment combinations, or geographic indicators (Afolabi, Chukwurah & Abieba, 2025, Chintoh et al., 2025, Oso et al., 2025). Furthermore, de-identification is often a one-time process, which does not account for future data linkages or technological advancements that could undermine previously effective protections. The dynamic and multi-dimensional nature of health data makes complete anonymization extremely difficult to guarantee over time. As such, a cautious approach must be adopted when sharing or utilizing de-identified data, balancing the benefits of data-driven research with the imperative to protect patient confidentiality.

The emergence of advanced technologies, particularly AI and IoT, introduces new layers of complexity and risk to EHR privacy. AI-driven tools are increasingly being used to assist in diagnosis, predict health risks, personalize treatment plans, and analyze population health trends. These systems rely on massive volumes of health data to train algorithms and improve performance (Adepoju et al., 2024, Chintoh et al., 2024, Sule et al., 2024). However, the use of AI raises important questions about how data is sourced, who has access to it, and how it is processed. Unlike traditional data use, AI systems may extract latent patterns and insights that were not initially evident or intended, raising concerns about unintended consequences, bias, and the potential misuse of sensitive information. Moreover, AI algorithms often operate as “black boxes,” making it difficult for patients and even clinicians to understand how decisions are being made or what data is being utilized (Alli & Dada, 2023, Hussain et al., 2023). This lack of transparency can erode trust and lead to skepticism about the fairness and integrity of AI-enabled healthcare tools.

The proliferation of IoT devices in healthcare—including wearable fitness trackers, smart medical implants, remote monitoring systems, and mobile health applications—further expands the privacy risk landscape. These devices continuously collect and transmit health-related data, often outside of traditional clinical settings, and frequently without explicit or ongoing patient consent (Atta et al., 2021, Dirlikov, 2021). Many of these devices are not subject to the same regulatory scrutiny as certified medical technologies, meaning they may lack robust privacy protections, encryption standards, or data governance policies. Data from IoT devices is often stored in cloud platforms or shared with third-party vendors, creating additional risk vectors and raising concerns about who has access to the information and how it is being monetized or repurposed.

The integration of IoT data into EHR systems also presents significant privacy management challenges. For instance, how should consent be managed when data is being collected in real-time from a wearable device and automatically synced with a patient's medical record? What safeguards exist to prevent unauthorized third parties—such as insurance companies or employers—from using this data to make discriminatory decisions? The answers to these questions remain unclear, and current regulatory frameworks often lag behind technological innovation, leaving gaps in protection (Ayo-Farai et al.. 2023, Babarinde et al., 2023).

As EHR systems evolve and embrace these emerging technologies, there is an urgent need to revisit and strengthen privacy protections across all levels. This includes updating consent models to accommodate dynamic and real-time data flows, developing privacy-preserving machine learning techniques that minimize exposure to raw data, and enforcing stricter accountability for data handling by third-party vendors (Adepoju et al., 2022, Opia, Matthew & Matthew, 2022). Additionally, privacy impact assessments should become standard practice in the development and deployment of AI and IoT solutions in healthcare, ensuring that potential risks are identified and mitigated before widespread implementation.

In summary, the privacy concerns surrounding Electronic Health Records are multifaceted and increasingly influenced by the integration of advanced technologies and shifting data paradigms. While EHRs offer significant benefits in improving care delivery and health outcomes, they also require robust privacy safeguards to protect the rights and interests of patients. Ensuring patient consent and control, improving data de-identification techniques, and addressing the implications of AI and IoT are central to maintaining trust in digital healthcare systems (Jahun et al., 2021, Ogbeta, Mbata & Udemezue, 2021). As healthcare continues to innovate, privacy must remain a foundational pillar, supported by adaptive policies, transparent practices, and technology solutions designed with security and ethics in mind.

5. REGULATORY COMPLIANCE LANDSCAPE

The regulatory compliance landscape surrounding Electronic Health Records (EHRs) is both expansive and evolving, shaped by regional, national, and international laws aimed at protecting the privacy, integrity, and security of sensitive health information. As EHR systems become the norm across global healthcare infrastructures, ensuring adherence to these regulations has emerged as a critical priority for healthcare providers, technology vendors, and policymakers alike (Afolabi, Chukwurah & Abieba, 2025, Edwards et al., 2025). The compliance environment, however, is increasingly complex—marked by varying legal standards, dynamic technological changes, and the continuous challenge of aligning operational practices with legal mandates. A comprehensive understanding of these regulatory frameworks and their implementation challenges is essential to addressing current security and privacy issues within EHR systems and charting a path toward more robust data governance.

Among the most well-established and widely referenced regulatory frameworks is the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Enacted in 1996 and supplemented by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, HIPAA sets national standards for the protection of individually identifiable health information (Azubuike et al., 2024, Chintoh et al., 2024, Odionu et al., 2024). It mandates safeguards for the confidentiality, integrity, and availability of electronic protected health information (ePHI), while also establishing rules for breach notification, access control, and penalties for non-compliance.

HIPAA's Security Rule, in particular, provides specific guidelines on administrative, physical, and technical safeguards, including encryption, access control, audit controls, and user authentication.

In the European Union, the General Data Protection Regulation (GDPR), which took effect in May 2018, has dramatically reshaped the global conversation around data privacy, including in the context of healthcare. GDPR offers broader protections than HIPAA, applying not only to healthcare entities but to all organizations processing the personal data of EU residents. It emphasizes principles such as data minimization, purpose limitation, and the right to be forgotten, while placing stringent requirements on data controllers and processors for consent, data transfer, and breach notification (Adelodun & Anyanwu, 2025, Ibeh et al., 2025, Oso et al., 2025). One key distinction is that GDPR views health data as a special category of personal data, warranting heightened protection and explicit consent for processing.

Beyond HIPAA and GDPR, numerous other regional and national regulations influence EHR compliance efforts. For instance, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and various provincial health privacy laws govern the use and disclosure of health data. Australia's Privacy Act and the My Health Records Act establish requirements for handling digital health records (Adepoju et al., 2023, Balogun et al., 2023). In Asia, countries such as Singapore, Japan, and South Korea have enacted their own privacy and health information protection laws, while other regions, including parts of Africa and the Middle East, are developing or strengthening their regulatory frameworks. The diversity of these regulations poses a significant challenge for global health organizations, particularly those that engage in cross-border data exchange or manage multinational operations.

Implementing regulatory compliance in the context of EHRs involves navigating several operational challenges. One major issue is interoperability—the ability of disparate health IT systems to share and use information effectively. While interoperability is essential for coordinated care and improved health outcomes, it also raises substantial compliance concerns, especially when data moves across organizational or national boundaries (Adelodun & Anyanwu, 2024, Kelvin-Agwu et al., 2024, Olorunsogo et al., 2024). Different jurisdictions may impose conflicting requirements for consent, data storage, and transfer protocols. For example, data that is compliant under HIPAA in the United States may not meet GDPR standards in the European Union, particularly regarding consent granularity or data subject rights. This tension complicates data sharing between research institutions, multinational healthcare providers, and international public health collaborations (Alli & Dada, 2022, Ige et al., 2022).

Another persistent challenge lies in maintaining comprehensive audit trails and meeting documentation requirements. Regulatory frameworks typically require detailed logs of access, modifications, disclosures, and security events related to patient data. These audit trails are critical for detecting unauthorized access, ensuring accountability, and demonstrating compliance during investigations or audits (Austin-Gabriel et al., 2021, Dirlikov et al., 2021). However, maintaining and managing these logs can be resource-intensive, particularly for organizations with limited IT capacity or a high volume of data transactions. Moreover, the pressure to retain documentation for extended periods—sometimes beyond the operational life of the systems generating them—creates storage and cost burdens that many healthcare institutions struggle to manage.

The consequences of non-compliance with data protection regulations are not merely theoretical; they are regularly illustrated through high-profile case studies that underscore the real-world implications of lapses in EHR governance.

One notable case involved Anthem Inc., one of the largest health insurance companies in the United States, which suffered a massive data breach in 2015 affecting nearly 80 million individuals. Attackers accessed names, birthdates, social security numbers, and medical Ids (Ayo-Farai et al., 2023, Ikwuanusi, Adepoju & Odionu, 2023). The breach was attributed to inadequate cybersecurity controls and a failure to implement multi-factor authentication. As a result, Anthem agreed to a $16 million settlement with the U.S. Department of Health and Human Services (HHS)—the largest HIPAA enforcement action at the time—along with additional penalties from state regulators.

In another case, the UK's National Health Service (NHS) experienced widespread disruption in 2017 due to the WannaCry ransomware attack, which affected dozens of hospitals and led to canceled appointments, delayed surgeries, and the exposure of patient records. Although not a targeted health data breach per se, the incident revealed critical vulnerabilities in legacy IT infrastructure and highlighted the NHS's failure to apply timely software updates—a requirement that falls under many regulatory and cybersecurity frameworks (Adepoju et al., 2023, Ike et al., 2023). The event prompted renewed investment in NHS digital resilience and called attention to the risks associated with underfunded healthcare IT systems.

The GDPR has also seen notable enforcement actions. In 2020, Haga Hospital in the Netherlands was fined €460,000 by the Dutch Data Protection Authority after it was found that unauthorized hospital staff accessed the medical records of a well-known patient without appropriate safeguards in place. The incident underscored the importance of implementing effective role-based access controls and real-time monitoring systems—principles that are also core to HIPAA and other privacy regulations (Adaramola et al., 2024, Kelvin-Agwu et al., 2024, Temedie-Asogwa et al., 2024). Similarly, in Finland, a mental health services provider known as Vastaamo faced public outrage and legal action after hackers stole therapy session notes and attempted to extort both the clinic and individual patients. The scandal raised questions about encryption practices, breach notification protocols, and organizational transparency.

These case studies demonstrate not only the financial and reputational costs of non-compliance but also the emotional and psychological toll on patients whose private health information is compromised. They reinforce the notion that compliance must be more than a box-ticking exercise; it must be integrated into the fabric of organizational culture and supported by robust technical, administrative, and legal frameworks (Afolabi, Chukwurah & Abieba, 2025, Odionu et al., 2025). This includes conducting regular risk assessments, updating policies in line with evolving threats and regulations, and fostering a culture of accountability and privacy consciousness among all staff.

Looking ahead, the regulatory landscape is likely to become even more demanding as new technologies—such as artificial intelligence, genomic data analysis, and telehealth platforms—reshape the healthcare ecosystem. Regulators around the world are beginning to explore additional layers of oversight for these emerging domains, including AI ethics guidelines, data protection impact assessments, and algorithmic transparency requirements. For organizations managing EHR systems, staying ahead of these developments will require proactive engagement with regulators, participation in policy development, and the continuous adaptation of compliance strategies to meet the demands of a digitally connected and data-rich healthcare future (Ayanbode et al., 2024, Majebi, Adelodun, & Anyanwu, 2024, Zouo & Olamijuwon, 2024).

In conclusion, the regulatory compliance landscape for EHR systems is marked by an intricate web of local and global laws, implementation challenges, and the constant threat of data breaches. Adhering to frameworks like HIPAA, GDPR, and regional policies requires not only technical safeguards but also organizational commitment to privacy and accountability. As healthcare continues its digital transformation, the ability to navigate this evolving compliance terrain will be crucial in ensuring that electronic health records fulfill their promise of enhancing patient care without compromising trust or security (Ayo-Farai et al., 2024, Oddie-Okeke et al., 2024, Uwumiro et al., 2024).

6. CURRENT MITIGATION STRATEGIES

Mitigating the security, privacy, and compliance challenges associated with Electronic Health Records (EHRs) is a critical priority for healthcare providers and institutions worldwide. As EHRs serve as central repositories for sensitive patient information, their protection requires a multi-layered, proactive, and adaptive strategy that addresses both technological and human vulnerabilities (Adepoju et al., 2023, Balogun et al., 2023. Current mitigation efforts in the healthcare sector have evolved to incorporate a range of defensive mechanisms—technical, procedural, and behavioral—that work in tandem to safeguard patient data from external threats, internal misuse, and accidental exposure. Among these, encryption, access control, multi-factor authentication, intrusion detection systems, and comprehensive staff training programs are key components of modern EHR protection frameworks.

One of the most fundamental and widely adopted strategies for securing EHR systems is encryption. Encryption transforms readable data into an unreadable format using cryptographic algorithms, ensuring that unauthorized parties cannot access or interpret sensitive information even if they manage to breach the system. In the context of EHRs, encryption is typically applied at two levels: data at rest and data in transit (Ayo-Farai et al., 2024, Odionu et al., 2024, Olowe et al., 2024). Data at rest refers to stored information in databases, servers, or storage devices, while data in transit encompasses information being transmitted between systems, such as during communication between a healthcare provider and a cloud-based EHR platform. The implementation of strong encryption protocols—such as Advanced Encryption Standard (AES) for data at rest and Transport Layer Security (TLS) for data in transit—is essential to maintaining the confidentiality and integrity of patient records (Adelodun & Anyanwu, 2024, Kelvin-Agwu et al., 2024).

Encryption is most effective when paired with robust access control mechanisms that ensure only authorized users can view or manipulate specific types of health data. Access control in EHR systems is commonly enforced through role-based access control (RBAC), which assigns user permissions based on job responsibilities. For example, a physician may have access to full patient records, while administrative staff are limited to demographic or billing information (Alli & Dada, 2024, Fasipe & Ogunboye, 2024, Ogundairo et al., 2024). Fine-grained access control enables healthcare organizations to implement the principle of least privilege, reducing the risk of unauthorized access and mitigating the potential damage from insider threats. Moreover, access logs and audit trails are maintained to monitor user activity, detect suspicious behavior, and support compliance with regulatory requirements (Ayinde et al., 2021, Hussain et al., 2021).

Despite the benefits of access control and encryption, single-factor authentication methods—such as username and password combinations—remain a weak link in many EHR security frameworks. Passwords are vulnerable to phishing attacks, brute-force attempts, and social engineering, making it imperative to strengthen identity verification through multi-factor authentication (MFA).

MFA adds an extra layer of security by requiring users to present two or more credentials to verify their identity (Adepoju et al., 2023, Ezeamii et al., 2023). These credentials typically fall into three categories: something the user knows (password or PIN), something the user has (security token or mobile device), and something the user is (biometric data like fingerprints or facial recognition).

In the healthcare sector, MFA is increasingly being adopted to secure access to EHR systems, especially for remote access or sensitive administrative functions. For example, clinicians accessing EHRs from off-site locations may be required to input a one-time code sent to their registered device or perform biometric verification. MFA significantly reduces the likelihood of unauthorized access, even if login credentials are compromised (Adegoke et al., 2022, Patel et al., 2022). However, its implementation must be carefully managed to balance security with user convenience, particularly in fast-paced clinical environments where ease of access is vital.

Another important line of defense against cyber threats is the deployment of intrusion detection systems (IDS). IDS solutions monitor network traffic, system behavior, and user activity for signs of malicious or anomalous behavior. These systems use a combination of signature-based and anomaly-based detection methods. Signature-based detection compares activity against known patterns of malicious behavior, while anomaly-based detection uses machine learning to establish baseline behavior and flag deviations (Afolabi et al., 2023, Ikwuanusi, Adepoju & Odionu, 2023). In healthcare environments, IDS tools can alert administrators to potential threats such as unauthorized access attempts, unusual login patterns, or attempts to exfiltrate large volumes of data.

When integrated with security information and event management (SIEM) platforms, IDS tools provide real-time alerts and forensic capabilities that are crucial for incident response and regulatory compliance. For instance, in the event of a data breach, IDS logs can help trace the source of the intrusion, assess the extent of the damage, and support notification requirements under regulations like HIPAA or GDPR. However, the effectiveness of IDS depends on proper configuration, continuous monitoring, and timely response (Adepoju et al., 2023, Nnagha et al.,2023). False positives and alert fatigue are common challenges, requiring skilled personnel and clear protocols to distinguish between benign and harmful events.

While technical controls are essential, they are insufficient on their own to secure EHR systems. Human factors often represent the weakest link in the security chain, making staff training and cybersecurity awareness indispensable components of any comprehensive mitigation strategy. Many security breaches occur due to human error, such as employees falling victim to phishing emails, mishandling portable devices, or inadvertently sharing sensitive information (Ajayi et al., 2024, Ezeamii et al., 2024, Ohalete et al., 2024). Regular training programs can educate staff about the importance of cybersecurity, common threat vectors, and best practices for protecting patient data.

Effective training should be role-specific, providing tailored guidance for different user groups such as clinicians, administrative staff, IT personnel, and executives. Training sessions should cover topics like recognizing phishing attempts, proper password management, secure data sharing practices, and protocols for reporting suspicious activity. Interactive and scenario-based learning can enhance engagement and retention, while simulated phishing campaigns can test employees' vigilance in real-world conditions.

Furthermore, cybersecurity awareness should not be a one-time effort but an ongoing initiative reinforced through newsletters, refresher courses, and visible leadership support (Adelodun & Anyanwu, 2024, Kelvin-Agwu et al., 2024, Zouo & Olamijuwon, 2024).

Creating a culture of security awareness also involves establishing clear policies and accountability structures. Employees should understand not only how to protect data but also the consequences of failing to do so. Healthcare organizations must ensure that data protection responsibilities are clearly defined and that staff know whom to contact in the event of a suspected breach or security incident. Regular audits, compliance checks, and internal reviews can reinforce adherence to policies and highlight areas for improvement (Adepoju et al., 2023, Nwaonumah et al., 2023).

Together, these mitigation strategies form a layered defense-in-depth approach that significantly enhances the security posture of EHR systems. Encryption and access control protect the data itself and restrict unauthorized access. Multi-factor authentication strengthens identity verification and reduces the impact of credential theft. Intrusion detection systems provide real-time monitoring and alerting to quickly identify and respond to emerging threats. Staff training and cybersecurity awareness address the human element, ensuring that users act as vigilant defenders rather than inadvertent enablers of security breaches (Adelodun & Anyanwu, 2025, Ige et al., 2025).

Despite their effectiveness, these strategies must continuously evolve in response to new technologies, emerging threats, and regulatory developments. As healthcare organizations adopt cloud computing, telemedicine, artificial intelligence, and Internet of Things (IoT) devices, new vulnerabilities will emerge that challenge existing safeguards (Alli & Dada, 2023, Majebi et al., 2023). Future mitigation efforts must therefore emphasize adaptability, integration, and collaboration across technical, organizational, and policy domains. By remaining vigilant and proactive, healthcare providers can build resilient EHR systems that uphold the trust of patients, support regulatory compliance, and protect the confidentiality, integrity, and availability of health data in an increasingly digital world (Adepoju et al., 2023, Ogbeta et al., 2023).

7. EMERGING TECHNOLOGIES AND FUTURE DIRECTIONS

As the landscape of healthcare technology continues to evolve, so too do the strategies and tools needed to secure Electronic Health Records (EHRs), protect patient privacy, and ensure regulatory compliance. Traditional mitigation approaches such as encryption, access controls, and staff training remain foundational, but they must now be augmented by emerging technologies that offer more resilient, adaptive, and scalable solutions (Adekola et al., 2023, Ezeamii et al., 2023). In response to increasingly sophisticated cyber threats, growing volumes of sensitive health data, and the demands of cross-border data sharing, healthcare systems are exploring innovative avenues such as blockchain, federated learning, differential privacy, real-time monitoring, and policy harmonization (Ajayi et al., 2025, Ogbeta, Mbata & Udemezue, 2025). These advancements represent not just technical progress but a broader shift toward smarter, more integrated systems that can anticipate and respond to both operational and ethical challenges in managing EHRs.

One of the most promising developments in the realm of data integrity and accountability is the use of blockchain technology for immutable logging. Blockchain, a decentralized ledger system, offers a transparent, tamper-proof method of recording data transactions.

In the context of EHRs, blockchain can be used to log access and modifications to health records, providing a traceable and auditable trail that cannot be altered retroactively (Adepoju et al., 2024, Kelvin-Agwu et al., 2024, Shittu et al., 2024). This immutability enhances trust, as patients and providers alike can be assured that the history of data access is secure and verifiable. Unlike traditional centralized logging systems, which can be susceptible to insider manipulation or external breaches, blockchain's distributed nature ensures redundancy and resistance to unauthorized changes (Adelodun & Anyanwu, 2024, Majebi, Adelodun & Anyanwu, 2024). Additionally, smart contracts can be programmed into blockchain networks to automatically enforce access permissions or trigger alerts when predefined rules are violated. These features make blockchain particularly well-suited to addressing concerns related to auditability, transparency, and long-term data stewardship in healthcare environments (Alli & Dada, 2023, Fagbule et al., 2023).

However, blockchain's implementation in EHR systems is not without challenges. Issues such as scalability, latency, and integration with existing systems must be addressed to make blockchain a practical solution for high-volume healthcare networks. Moreover, storing actual health data on a blockchain is generally discouraged due to privacy and storage limitations; instead, hashed references or metadata are stored on-chain, with the actual records maintained in secure, off-chain databases (Adepoju et al., 2024, Ezeamii et al., 2024, Okhawere et al., 2024). Despite these challenges, pilot projects and research initiatives around the world continue to explore blockchain's potential in healthcare, particularly for managing consent, verifying provider credentials, and enabling secure health information exchanges.

In parallel with blockchain, another transformative innovation gaining momentum is the application of federated learning and differential privacy in the development of EHR-based analytics and artificial intelligence (AI) models. Traditional machine learning approaches require centralizing data in a single repository, which poses significant privacy and security risks (Adelodun et al., 2018, Ike et al., 2021). Federated learning addresses this issue by enabling AI models to be trained across multiple decentralized data sources—such as hospitals, clinics, or wearable devices—without transferring the raw data. Each participating node trains the model locally using its data and shares only model updates (e.g., weights and gradients) with a central aggregator. This method allows institutions to collaborate on machine learning projects without exposing sensitive patient information (Ajayi, Alozie & Abieba, 2025, Ekeh et al., 2025).

To further enhance privacy, federated learning is often combined with differential privacy, a technique that introduces mathematically calibrated noise into the data or model outputs to prevent re-identification of individuals. Differential privacy provides formal privacy guarantees, ensuring that the inclusion or exclusion of a single individual's data has a negligible impact on the model's predictions (Adepoju et al., 2024, Majebi, Adelodun & Anyanwu, 2024). Together, federated learning and differential privacy offer a powerful framework for privacy-preserving AI in healthcare, enabling innovations in diagnosis, risk prediction, and treatment personalization without compromising patient confidentiality.

These technologies also align well with current regulatory frameworks and emerging global data governance principles that emphasize data minimization, purpose limitation, and transparency. However, their practical deployment requires overcoming technical hurdles such as communication efficiency, model convergence, and trust management between participating institutions. Research into robust aggregation methods, adversarial defenses, and dynamic participation schemes is ongoing and will be critical to scaling these solutions across real-world healthcare ecosystems (Adelodun & Anyanwu, 2024, Obianyo et al., 2024, Olowe et al., 2024).

Another critical frontier in the advancement of EHR security is real-time monitoring and threat intelligence. While traditional security systems focus on perimeter defenses and retrospective audits, real-time monitoring enables healthcare organizations to detect, investigate, and respond to cyber threats as they occur. Advanced monitoring systems utilize behavioral analytics, anomaly detection, and machine learning algorithms to continuously analyze user activities, network traffic, and system logs (Anyanwu et al., 2024, Matthew et al., 2024, Okoro et al., 2024). These systems can identify deviations from normal patterns, such as unusual login times, excessive data downloads, or unauthorized access to sensitive patient files, and trigger immediate alerts or automated countermeasures.

Threat intelligence further enhances these capabilities by providing contextual information about emerging threats, vulnerabilities, and attacker behaviors sourced from external feeds, industry reports, and global security communities. Integrating threat intelligence with internal monitoring systems allows healthcare organizations to anticipate risks, adapt defenses, and respond more effectively to sophisticated attacks. Moreover, real-time visibility into system performance and security events supports compliance by ensuring that audit trails are complete, timely, and actionable (Alozie et al., 2024, Ezeamii et al., 2024, Okobi et al., 2024).

To fully realize the potential of real-time security, healthcare organizations must invest in technologies such as Security Information and Event Management (SIEM) platforms, Endpoint Detection and Response (EDR) tools, and automated orchestration systems. They must also establish dedicated Security Operations Centers (SOCs) or collaborate with managed security service providers (MSSPs) to maintain 24/7 vigilance. The combination of advanced analytics and human expertise ensures a proactive security posture that can keep pace with the evolving threat landscape.

Finally, the future of EHR security, privacy, and compliance must involve a concerted effort toward policy harmonization and global collaboration. As healthcare becomes more interconnected through telemedicine, international research collaborations, and global health initiatives, the ability to securely share health data across borders becomes increasingly important. However, regulatory fragmentation remains a significant obstacle. Laws such as HIPAA, GDPR, and various national privacy acts impose differing requirements for data protection, consent, and cross-border transfers (Adepoju et al., 2024, Kelvin-Agwu et al., 2024, Oladosu et al., 2024). These inconsistencies complicate compliance, hinder interoperability, and slow the adoption of innovative technologies.

To address these challenges, stakeholders must work toward the development of harmonized standards and frameworks that balance local sovereignty with global interoperability. Initiatives such as the Global Digital Health Partnership (GDHP), the World Health Organization's digital health strategy, and efforts by standards organizations like HL7 and ISO are steps in the right direction (Ogundairo et al., 2023, Uwumiro et al., 2023). These collaborations aim to promote shared principles, technical standards, and governance models that support secure, ethical, and efficient data use across jurisdictions.

Policy harmonization also requires engagement with diverse stakeholders, including governments, healthcare providers, technology vendors, patients, and civil society. Inclusive dialogue and participatory policy development can help align regulatory objectives with technological capabilities and societal values (Akinade et al., 2022, Patel et al., 2022).

In addition, mechanisms for cross-border data sharing—such as data trusts, federated registries, and secure data enclaves—should be explored and standardized to support collaborative research, public health surveillance, and emergency response efforts without compromising privacy or security.

In conclusion, emerging technologies and forward-looking strategies are reshaping how healthcare systems protect EHRs and uphold patient trust in a rapidly digitizing world. Blockchain provides a foundation for immutable, transparent data logging; federated learning and differential privacy offer privacy-preserving pathways to AI innovation; real-time monitoring and threat intelligence enable proactive defense against cyber threats; and policy harmonization paves the way for secure, ethical global data exchange (Akinade et al., 2021, Bidemi et al., 2021). While these technologies present implementation challenges, their potential to strengthen security, enhance privacy, and support compliance is undeniable. As healthcare continues its digital transformation, embracing these innovations will be essential to building a future where electronic health information is both powerful and protected (Adepoju et al., 2025, Amafah et al., 2025, Ige et al., 2025)

8. DISCUSSION

The systematic review of security, privacy, and compliance challenges in Electronic Health Records (EHRs) reveals a complex and evolving landscape where technological advancement must be continuously balanced with ethical obligations, regulatory mandates, and operational realities. Through the comprehensive examination of current practices, frameworks, and innovations, the review presents several critical insights that not only underscore the progress made but also highlight persistent vulnerabilities and emerging risks (Ajayi, Alozie & Abieba, 2025, Ekeh et al., 2025). These insights serve as a call to action for healthcare stakeholders—governments, healthcare providers, technology vendors, researchers, and patients—to collaboratively address the multifaceted challenges associated with safeguarding sensitive health information in digital ecosystems.

One of the most prominent insights from the review is the central role that EHRs now play in modern healthcare delivery. With increasing digitization, EHR systems have become indispensable tools for storing, sharing, and managing patient information. They enable real-time access to clinical data, support continuity of care, improve diagnostic accuracy, and streamline administrative processes (Anyanwu et al., 2024, Majebi, Adelodun & Anyanwu, 2024). However, the growing dependence on EHRs also increases the risk exposure to a variety of threats. From sophisticated cyberattacks such as ransomware and phishing to insider threats and unintentional data leaks, the surface area for security breaches has expanded significantly. The review confirms that despite the implementation of standard protective measures—encryption, access control, audit trails, and multi-factor authentication—security breaches continue to occur, often exploiting human factors, legacy systems, or configuration gaps.

Another important finding is the increasing sophistication of threat actors targeting EHR systems. Healthcare data is uniquely valuable on the black market, as it can be used not only for identity theft and insurance fraud but also for blackmail or social engineering. Attackers are becoming more organized and well-funded, leveraging advanced tools and techniques to penetrate healthcare infrastructure. At the same time, many healthcare organizations lack the resources or expertise to deploy and maintain cutting-edge cybersecurity solutions.

Smaller providers, in particular, face disproportionate challenges due to limited IT budgets, aging hardware, and insufficient staff training (Adepoju et al., 2024, Kelvin-Agwu et al., 2024, Olowe et al., 2024). This disparity creates a security gap that adversaries can exploit, particularly in under-resourced healthcare settings.

The review also brings attention to the persistent tension between data utility and patient privacy. While EHRs are essential for clinical decision-making and increasingly for research and population health management, the use of personal health data raises ethical and legal concerns. Patients often remain unaware of how their data is collected, shared, or used, particularly when it involves secondary applications such as algorithm training or public health surveillance (Adelodun & Anyanwu, 2024, Ezeamii et al., 2024, Okoro et al., 2024). Consent models in many healthcare systems are outdated or inadequately implemented, resulting in broad, blanket consents that do not allow patients to exercise meaningful control over their information. Furthermore, although anonymization and de-identification techniques are widely used to protect privacy, the review highlights their limitations. Re-identification remains a real threat, especially when datasets are combined with external information sources or when rare conditions make individuals uniquely identifiable.

In examining compliance frameworks, the review outlines the fragmentation and inconsistency of global regulatory environments. While regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the General Data Protection Regulation (GDPR) in the European Union have established critical baselines for data protection, there is a lack of global harmonization (Al Zoubi,et al., 2022). This inconsistency creates barriers to cross-border data sharing, complicates research collaborations, and increases the burden on multinational healthcare organizations that must comply with multiple, sometimes conflicting, legal regimes. Moreover, compliance is not simply a matter of legal conformity—it requires continuous monitoring, documentation, and adaptation, which are often overlooked or under-resourced.

Despite these valuable findings, the review identifies several key gaps in both the literature and current practice. First, there is a limited body of empirical research evaluating the real-world effectiveness of implemented security and privacy controls in healthcare environments. Much of the existing literature focuses on theoretical models, conceptual frameworks, or retrospective breach analyses, but few studies provide longitudinal assessments or controlled evaluations of mitigation strategies (Matthew et al., 2021, Oladosu et al., 2021). Without such evidence, it remains difficult to determine which practices offer the greatest return on investment or how interventions should be prioritized in resource-constrained settings.

Second, there is a lack of comprehensive studies on the human factors influencing EHR security. While human error is often cited as a major cause of data breaches, there is insufficient understanding of the behavioral, cultural, and organizational determinants that contribute to risky practices. Research in this area could inform the design of more effective training programs, interface designs, and accountability mechanisms (Akinade et al., 2025, Ekeh, et al., 2025). Similarly, more research is needed on patient perceptions of privacy and consent in the digital age. Understanding how different populations perceive data ownership, risk, and trust can help tailor policies and communication strategies to enhance transparency and engagement.

Third, the review finds that emerging technologies such as artificial intelligence, machine learning, and Internet of Things (IoT) devices are rapidly transforming healthcare, yet regulatory frameworks and risk management practices have not kept pace.

These technologies introduce new vulnerabilities, including algorithmic bias, data leakage from interconnected devices, and opaque decision-making processes (Ogunboye et al., 2023, Ogundairo et al., 2023). However, they are often deployed without comprehensive privacy impact assessments or integration into organizational governance structures. This gap presents an urgent need for updated standards, interdisciplinary research, and proactive policy development.

The implications of these findings are significant for policy and research. From a policy perspective, there is a need for more cohesive, forward-looking regulatory frameworks that can adapt to technological change and support secure, ethical innovation. Policymakers should prioritize the harmonization of international privacy laws, the development of standardized consent mechanisms, and the enforcement of minimum cybersecurity standards across all healthcare providers (Adepoju et al., 2022). Regulations must also be sensitive to the needs of smaller institutions and include provisions for capacity building and financial support to close the digital divide.

At the organizational level, healthcare institutions must move beyond compliance checklists and adopt a culture of security and privacy. This includes investing in continuous risk assessments, adopting best practices in cybersecurity, and embedding privacy by design principles into EHR systems. Institutions should also engage patients as active stakeholders in their data stewardship, providing clear information about how their data is used and offering tools for granular consent and access control (Adelodun & Anyanwu, 2025, Ogbeta, Mbata & Udemezue, 2025).

From a research standpoint, there is a pressing need for interdisciplinary collaboration among technologists, clinicians, ethicists, legal scholars, and social scientists. Research agendas should focus on evaluating the real-world impact of security interventions, exploring the sociotechnical dimensions of privacy, and developing scalable, privacy-preserving technologies. Efforts should also be made to build open-access datasets and benchmarks that can facilitate comparative analysis and foster innovation in privacy-enhancing solutions (Al Hasan, Matthew & Toriola, 2024, Bello et al., 2024, Olowe et al., 2024).

In conclusion, the systematic review provides a nuanced and comprehensive understanding of the security, privacy, and compliance challenges in EHR systems. It reveals a landscape marked by technological progress but constrained by uneven implementation, regulatory fragmentation, and persistent vulnerabilities (Akinade et al., 2025, Ekeh et al., 2025). While significant strides have been made in developing safeguards and establishing legal protections, critical gaps remain—particularly in the areas of consent, human factors, empirical evaluation, and preparedness for emerging technologies. Addressing these challenges will require coordinated efforts across policy, practice, and research. Only through sustained and inclusive collaboration can we build a digital health ecosystem that truly protects patients while enabling the transformative potential of electronic health records (Adepoju et al., 2024, Balogun et al., 2024, Okon, Zouo & Sobowale, 2024).

9. CONCLUSION

The systematic review of security, privacy, and compliance challenges in Electronic Health Records (EHRs) underscores the immense value and complexity of safeguarding digital health information in a rapidly evolving technological landscape. EHRs have transformed healthcare delivery by improving data accessibility, enhancing care coordination, and enabling data-driven clinical decisions. However, they also introduce significant risks related to cybersecurity, patient privacy, and regulatory compliance.

The review highlights that while considerable progress has been made in implementing foundational safeguards—such as encryption, access control, and multi-factor authentication—these measures are not uniformly adopted or sufficient to counter the increasingly sophisticated threat landscape.

Key findings reveal that technical vulnerabilities, insider threats, and inadequate training continue to contribute to data breaches and privacy violations. The growing use of third-party applications, mobile health tools, and interconnected systems further complicates security management. Additionally, the limitations of current anonymization techniques, fragmented regulatory frameworks, and outdated consent models hinder effective data governance. Emerging technologies such as blockchain, federated learning, and real-time threat intelligence offer promising pathways for strengthening EHR protection, yet their integration into clinical practice and regulatory environments remains limited and uneven.

To address these challenges, the review recommends a multifaceted approach that combines technological innovation, policy development, and cultural change. Future research should focus on real-world evaluations of security measures, the behavioral dimensions of privacy practices, and the development of scalable, privacy-preserving solutions. Greater attention must also be paid to understanding patient expectations and building systems that support informed, meaningful consent. On the policy front, efforts should prioritize harmonizing global data protection laws, simplifying compliance requirements, and incentivizing best practices across healthcare settings.

In practice, healthcare organizations must move toward proactive, risk-based strategies that embed security and privacy into the design of all health IT systems. This includes fostering a culture of cybersecurity awareness, enhancing workforce training, and ensuring ongoing investment in advanced monitoring and detection tools. Collaboration across sectors—combining the expertise of clinicians, technologists, policymakers, and patients—is essential for building trust and resilience in the digital health ecosystem. As EHRs continue to shape the future of healthcare, securing them must remain a foundational priority to ensure that the benefits of digital innovation do not come at the expense of patient rights and data integrity.

References

[1] Abieba, O. A., Alozie, C. E., & Ajayi, O. O. (2025). Enhancing disaster recovery and business continuity in cloud environments through infrastructure as code. *Journal of Engineering Research and Reports, 27*(3), 127-136.

[2] Adaramola, T. S., Omole, O. M., Wada, I., Nwariaku, H., Arowolo, M. E., & Adigun, O. A. (2024). Internet of thing integration in green fintech for enhanced resource management in smart cities. *World Journal of Advanced Research and Reviews*, *23*(2), 1317-1327.

[3] Adegoke, S. A., Oladimeji, O. I., Akinlosotu, M. A., Akinwumi, A. I., & Matthew, K. A. (2022). HemoTypeSC point-of-care testing shows high sensitivity with alkaline cellulose acetate hemoglobin electrophoresis for screening hemoglobin SS and SC genotypes. *Hematology, Transfusion and Cell Therapy*, *44*(3), 341-345.

[4] Adekola, A.D., Alli, O.I., Mbata, A.O. & Ogbeta, C.P., 2023. Integrating multisectoral strategies for tobacco control: Evidence-based approaches and public health outcomes. International Journal of Medical and All Body Health Research, 4(1), pp.60-69. DOI: https://doi.org/10.54660/IJMBHR.2024.4.1.60-69.

[5] Adekola, A.D., Alli, O.I., Mbata, A.O., & Ogbeta, C.P. (2023) 'Integrating multisectoral strategies for tobacco control: evidence-based approaches and public health outcomes', International Journal of Medical and All Body Health Research, 4(1), pp. 60-69. Available at: https://doi.org/10.54660/IJMBHR.2024.4.1.60-69

[6] Adelodun, A. M., Adekanmi, A. J., Roberts, A., & Adeyinka, A. O. (2018). Effect of asymptomatic malaria parasitemia on the uterine and umbilical artery blood flow impedance in third-trimester singleton Southwestern Nigerian pregnant women. *Tropical Journal of Obstetrics and Gynaecology*, *35*(3), 333-341.

[7] Adelodun, M. O., & Anyanwu, E. C. (2024). A critical review of public health policies for radiation protection and safety.

[8] Adelodun, M. O., & Anyanwu, E. C. (2024). Environmental and patient safety: Advances in radiological techniques to reduce radiation exposure.

[9] Adelodun, M. O., & Anyanwu, E. C. (2024). Evaluating the environmental impact of Innovative Radiation Therapy Techniques in cancer treatment.

[10] Adelodun, M. O., & Anyanwu, E. C. (2024). Evaluating the environmental impact of innovative radiation therapy techniques in cancer treatment.

[11] Adelodun, M. O., & Anyanwu, E. C. (2024). Global Standards in Radiation Safety: A Comparative Analysis of Healthcare Regulations.

[12] Adelodun, M. O., & Anyanwu, E. C. (2024). Health Effects of Radiation: An Epidemiological Study on Populations Near Nuclear Medicine Facilities. *Health*, *13*(9), 228-239.

[13] Adelodun, M. O., & Anyanwu, E. C. (2024). Integrating Radiological Technology in environmental health surveillance to enhance public safety.

[14] Adelodun, M. O., & Anyanwu, E. C. (2025). Public Health Risks Associated with Environmental Radiation from Improper Medical Waste Disposal.

[15] Adelodun, M. O., & Anyanwu, E. C. (2025). Recent Advances in Diagnostic Radiation and Proposals for Future Public Health Studies.

[16] Adelodun, M., & Anyanwu, E. (2024). Comprehensive risk management and safety strategies in radiation use in medical imaging. *Int J Front Med Surg Res*, *6*.

[17] Adeloduna, M. O., & Anyanwub, E. C. (2025). Telehealth implementation: a review of project management practices and outcomes.

[18] Adeniyi, A., Arowoogun, J., Chidi, R., Okolo, C., & Babawarun, O. (2024). The Impact of electronic health records on Patient Care and Outcomes: a comprehensive review. World Journal of Advanced Research and Reviews, 21(2), 1446-1455. https://doi.org/10.30574/wjarr.2024.21.2.0592

[19] Adepoju, P. A., Adeola, S., Ige, B., Chukwuemeka, C., Oladipupo Amoo, O., & Adeoye, N. (2023). AI-driven security for next-generation data centers: Conceptualizing autonomous threat detection and response in cloud-connected environments. *GSC Advanced Research and Reviews, 15*(2), 162–172. https://doi.org/10.30574/gscarr.2023.15.2.0136

[20] Adepoju, P. A., Adeola, S., Ige, B., Chukwuemeka, C., Oladipupo Amoo, O., & Adeoye, N. (2022). Reimagining multi-cloud interoperability: A conceptual framework for seamless integration and security across cloud platforms. *Open Access Research Journal of Science and Technology, 4*(1), 071–082. https://doi.org/10.53022/oarjst.2022.4.1.0026

[21] Adepoju, P. A., Adeoye, N., Hussain, Y., Austin-Gabriel, B., & Ige, B. (2023). Geospatial AI and data analytics for satellite-based disaster prediction and risk assessment. *Open Access Research Journal of Engineering and Technology, 4*(2), 058–066. https://doi.org/10.53022/oarjet.2023.4.2.0058

[22] Adepoju, P. A., Akinade, A. O., Ige, A. B., & Afolabi, A. I. (2021). A conceptual model for network security automation: Leveraging AI-driven frameworks to enhance multi-vendor infrastructure resilience. *International Journal of Science and Technology Research Archive, 1*(1), 039–059. https://doi.org/10.53771/ijstra.2021.1.1.0034

[23] Adepoju, P. A., Akinade, A. O., Ige, A. B., & Afolabi, A. I. (2024). Cloud security challenges and solutions: A review of current best practices. *International Journal of Multidisciplinary Research and Growth Evaluation, 6*(1), 26–35. https://doi.org/10.54660/.ijmrge.2025.6.1.26-35

[24] Adepoju, P. A., Akinade, A. O., Ige, A. B., & Afolabi, A. I. (2024). Artificial intelligence in traffic management: A review of smart solutions and urban impact. *IRE Journals, 7*, Retrieved from https://www.irejournals.com/formatedpaper/1705886.pdf

[25] Adepoju, P. A., Akinade, A. O., Ige, A. B., Afolabi, A. I. (2023). A systematic review of cybersecurity issues in healthcare IT: Threats and solutions. *Iconic Research and Engineering Journals, 7*(10).

[26] Adepoju, P. A., Akinade, A. O., Ige, A. B., Afolabi, A. I., & Amoo, O. O. (2022). Advancing segment routing technology: A new model for scalable and low-latency IP/MPLS backbone optimization. *Open Access Research Journal of Science and Technology, 5*(2), 077–095. https://doi.org/10.53022/oarjst.2022.5.2.0056

[27] Adepoju, P. A., Akinade, A. O., Ige, B., & Adeoye, N. (2023). Evaluating AI and ML in cybersecurity: A USA and global perspective. *GSC Advanced Research and Reviews, 17*(1), 138–148. https://doi.org/10.30574/gscarr.2023.17.1.0409

[28] Adepoju, P. A., Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., & Afolabi, A. I. (2023). Natural language processing frameworks for real-time decision-making in cybersecurity and business analytics. *International Journal of Science and Technology Research Archive, 4*(2), 086–095. https://doi.org/10.53771/ijstra.2023.4.2.0018

[29] Adepoju, P. A., Austin-Gabriel, B., Ige, B., Hussain, Y., Amoo, O. O., & Adeoye, N. (2022). Machine Learning Innovations for Enhancing Quantum-resistant cryptographic protocols in Secure Communication. *Open Access Research Journal of Multidisciplinary Studies, 4*(1), 131–139. https://doi.org/10.53022/oarjms.2022.4.1.0075

[30] Adepoju, P. A., Chukwuemeka, C., Ige, B., Adeola, S., & Adeoye, N. (2024). Advancing Real-Time Decision-making frameworks using interactive dashboards for Crisis and Emergency Management. *International Journal of Management & Entrepreneurship Research, 6*(12), 3915–3950. https://doi.org/10.51594/ijmer.v6i12.1762

[31] Adepoju, P. A., Hussain, N. Y., Austin-Gabriel, B., & Afolabi, A. I., 2024. Data Science Approaches to Enhancing Decision-Making in Sustainable Development and Resource Optimization. International Journal of Engineering Research and Development, 20(12), pp.204-214.

[32] Adepoju, P. A., Hussain, Y., Austin-Gabriel, B., Ige, B., Amoo, O. O., & Adeoye, N. (2023). Generative AI advances for data-driven insights in IoT, cloud technologies, and big data challenges. *Open Access Research Journal of Multidisciplinary Studies, 6*(1), 051–059. https://doi.org/10.53022/oarjms.2023.6.1.0040

[33] Adepoju, P. A., Ige, A. B., Akinade, A. O., & Afolabi, A. I. (2024). Machine learning in industrial applications: An in-depth review and future directions. *International Journal of Multidisciplinary Research and Growth Evaluation, 6*(1), 36–44. https://doi.org/10.54660/.ijmrge.2025.6.1.36-44

[34] Adepoju, P. A., Ige, A. B., Akinade, A. O., & Afolabi, A. I. (2025). Smart Cities and Internet of Things (IoT): A Review of Emerging Technologies and Challenges. *International Journal of Research and Innovation in Social Science*, *9*(1), 1536-1549.

[35] Adepoju, P. A., Ike, C. C., Ige, A. B., Oladosu, S. A., & Afolabi, A. I. (2024). Advancing predictive analytics models for supply chain optimization in global trade systems. *International Journal of Applied Research in Social Sciences, 6*(12), 2929–2948. https://doi.org/10.51594/ijarss.v6i12.1769

[36] Adepoju, P. A., Ike, C. C., Ige, A. B., Oladosu, S. A., Amoo, O. O., & Afolabi, A. I. (2023). Advancing machine learning frameworks for customer retention and propensity modeling in E-Commerce platforms. *GSC Advanced Research and Reviews, 14*(2), 191–203. https://doi.org/10.30574/gscarr.2023.14.2.0017

[37] Adepoju, P. A., Oladosu, S. A., Ige, A. B., Ike, C. C., Amoo, O. O., & Afolabi, A. I. (2022). Next-generation network security: Conceptualizing a unified, AI-Powered Security Architecture for cloud-native and on-premise environments. *International Journal of Science and Technology Research Archive, 3*(2), 270–280. https://doi.org/10.53771/ijstra.2022.3.2.0143

[38] Adepoju, P. A., Sule, A. K., Ikwuanusi, U. F., Azubuike, C., & Odionu, C. S. (2024). Enterprise architecture principles for higher education: Bridging technology and stakeholder goals. International Journal of Applied Research in Social Sciences, 6(12), 2997-3009. https://doi.org/10.51594/ijarss.v6i12.1785

[39] Adewuyi, A. Y., Anyibama, B., Adebayo, K. B., Kalinzi, J. M., Adeniyi, S. A., & Wada, I. (2024). Precision agriculture: Leveraging data science for sustainable farming. *International Journal of Scientific Research Archive*, *12*(2), 1122-1129.

[40] Adhikari, A., Ezeamii, V., Ayo Farai, O., Savarese, M., & Gupta, J. (2024, August). Assessing Mold-Specific Volatile Organic Compounds and Molds Using Sorbent Tubes and a CDC/NIOSH developed tool in Hurricane Ian affected Homes. In *ISEE Conference Abstracts* (Vol. 2024, No. 1).

[41] Adhikari, A., Smallwood, S., Ezeamii, V., Biswas, P., Tasby, A., Nwaonumah, E., ... & Yin, J. (2024, August). Investigating Volatile Organic Compounds in Older Municipal Buildings and Testing a Green and Sustainable Method to Reduce Employee Workplace Exposures. In *ISEE Conference Abstracts* (Vol. 2024, No. 1).

[42] Adigun, O. A., Falola, B. O., Esebre, S. D., Wada, I., & Tunde, A. (2024). Enhancing carbon markets with fintech innovations: The role of artificial intelligence and blockchain. *World Journal of Advanced Research and Reviews*, *23*(2).

[43] Afolabi, A. I., Chukwurah, N., & Abieba, O. A. (2025). Agile Software Engineering Framework For Real-Time Personalization In Financial Applications.

[44] Afolabi, A. I., Chukwurah, N., & Abieba, O. A. (2025). Harnessing Machine Learning Techniques for Driving Sustainable Economic Growth and Market Efficiency.

[45] Afolabi, A. I., Chukwurah, N., & Abieba, O. A. (2025). Implementing cutting-edge software engineering practices for cross-functional team success.

[46] Afolabi, A. I., Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., & Adepoju, P. A., 2023. Geospatial AI and data analytics for satellite-based disaster prediction and risk assessment. Open Access Research Journal of Engineering and Technology, 04(02), pp.058-066.

[47] Ajayi, A. M., Omokanye, A. O., Olowu, O., Adeleye, A. O., Omole, O. M., & Wada, I. U. (2024). Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity.

[48] Ajayi, O. O., Alozie, C. E., & Abieba, O. A. (2025). Enhancing Cybersecurity in Energy Infrastructure: Strategies for Safeguarding Critical Systems in the Digital Age. *Trends in Renewable Energy*, *11*(2), 201-212.

[49] Ajayi, O. O., Alozie, C. E., & Abieba, O. A. (2025). Innovative cybersecurity strategies for business intelligence: Transforming data protection and driving competitive superiority. *Gulf Journal of Advance Business Research*, *3*(2), 527-536.

[50] Ajayi, O. O., Alozie, C. E., Abieba, O. A., Akerele, J. I., & Collins, A. (2025). Blockchain technology and cybersecurity in fintech: Opportunities and vulnerabilities. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*(1).

[51] Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2025). Cloud Security Challenges and Solutions: A Review of Current Best Practices.

[52] Akinade, A. O., Adepoju, P. A., Ige, A. B., Afolabi, A. I., & Amoo, O. O. (2021). A conceptual model for network security automation: Leveraging ai-driven frameworks to enhance multi-vendor infrastructure resilience.

[53] Akinade, A. O., Adepoju, P. A., Ige, A. B., Afolabi, A. I., & Amoo, O. O. (2022). Advancing segment routing technology: A new model for scalable and low-latency IP/MPLS backbone optimization.

[54] Al Hasan, S. M., Matthew, K. A., & Toriola, A. T. (2024). Education and mammographic breast density. *Breast Cancer Research and Treatment*, 1-8.

[55] Al Zoubi, M. A. M., Amafah, J., Temedie-Asogwa, T., & Atta, J. A. (2022). International Journal of Multidisciplinary Comprehensive Research.

[56] Alli, O. I. & Dada, S. A. (2023). Cross-Cultural tobacco dependency treatment: A robust review of models for tailored interventions in diverse healthcare contexts. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), pp. 1102–1108. DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.1102-1108

[57] Alli, O. I. & Dada, S. A. (2023). Cross-Cultural tobacco dependency treatment: A robust review of models for tailored interventions in diverse healthcare contexts. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), pp. 1102–1108. DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.1102-1108

[58] Alli, O. I. & Dada, S. A. (2023). Reducing maternal smoking through evidence-based interventions: Advances and emerging models in high-impact public health strategies. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), pp. 1095–1101. DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.1095-1101

[59] Alli, O. I., & Dada, S. A. (2024). Global advances in tobacco control policies: A review of evidence, implementation models, and public health outcomes. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), pp. 1456–1461. DOI: https://doi.org/10.54660/.IJMRGE.2024.5.6.1456-1461

[60] Alli, O.I. & Dada, S.A. (2021) 'Innovative models for tobacco dependency treatment: A review of advances in integrated care approaches in high-income healthcare systems', IRE Journals, 5(6), pp. 273-282. Available at: https://www.irejournals.com/

[61] Alli, O.I. & Dada, S.A., 2022. Pharmacist-led smoking cessation programs: A comprehensive review of effectiveness, implementation models, and future directions. International Journal of Science and Technology Research Archive, 3(2), pp.297–304. Available at: https://doi.org/10.53771/ijstra.2022.3.2.0129

[62] Alozie, C. E., Collins, A., Abieba, O. A., Akerele, J. I., & Ajayi, O. O. (2024). International Journal of Management and Organizational Research.

[63] Al-Zubaidie, M., Zhang, Z., & Zhang, J. (2019). Pax: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system. International Journal of Environmental Research and Public Health, 16(9), 1490. https://doi.org/10.3390/ijerph16091490

[64] Amafah, J., Temedie-Asogwa, T., Atta, J. A., & Al Zoubi, M. A. M. (2023). The Impacts of Treatment Summaries on Patient-Centered Communication and Quality of Care for Cancer Survivors.

[65] Anyanwu, E. C., Maduka, C. P., Ayo-Farai, O., Okongwu, C. C., & Daraojimba, A. I. (2024). Maternal and child health policy: A global review of current practices and future directions. *World Journal of Advanced Research and Reviews*, *21*(2), 1770-1781.

[66] Anyanwu, E. C., Okongwu, C. C., Olorunsogo, T. O., Ayo-Farai, O., Osasona, F., & Daraojimba, O. D. (2024). Artificial Intelligence In Healthcare: A Review Of Ethical Dilemmas And Practical Applications. *International Medical Science Research Journal*, *4*(2), 126-140.

[67] Ariyibi, K. O., Bello, O. F., Ekundayo, T. F., & Ishola, O. (2024). Leveraging Artificial Intelligence for enhanced tax fraud detection in modern fiscal systems.

[68] Atandero, M.O., Fasipe, O.J., Famakin, S.M. and Ogunboye, I., (2024). A cross-sectional survey of comorbidity profile among adult Human Immunodeficiency Virus-infected patients attending a Nigeria medical university teaching hospital campus located in Akure, Ondo State. Archives of Medicine and Health Sciences, [online] Available at: https://doi.org/10.4103/amhs.amhs_94_24.

[69] Atta, J. A., Al Zoubi, M. A. M., Temedie-Asogwa, T., & Amafah, J. (2021): Comparing the Cost-Effectiveness of Pharmaceutical vs. Non-Pharmaceutical Interventions for Diabetes Management.

[70] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Research Journal of Engineering and Technology*, *1*(1), 47-55.

[71] Ayanbode, N., Abieba, O. A., Chukwurah, N., Ajayi, O. O., & Ifesinachi, A. (2024). Human Factors in Fintech Cybersecurity: Addressing Insider Threats and Behavioral Risks.

[72] Ayinde, B.A., Owolabi, J.O., Uti, I.S., Ogbeta, P.C. & Choudhary, M.I., 2021. Isolation of the antidiarrhoeal tiliroside and its derivative from Waltheria indica leaf extract. Nigerian Journal of Natural Products and Medicine, 25, pp.86-90. DOI: https://dx.doi.org/10.4314/njnpm.v25i1.10.

[73] Ayo-Farai, O., Gupta, J., Ezeamii, V., Savarese, M., & Adhikari, A. (2024). Surface Microbial Activity in Hurricane Ian Affected Homes in Relation To Environmental Factors.

[74] Ayo-Farai, O., Jingjing, Y., Ezeamii, V., Obianyo, C., & Tasby, A. (2024). Impacts on Indoor Plants on Surface Microbial Activity in Public Office Buildings in Statesboro Georgia.

[75] Ayo-Farai, O., Momodu, P. A., Okoye, I. C., Ekarika, E., Okafor, I. T., & Okobi, O. E. (2024). Analyzing Knowledge Status and HIV Linkage to Care: Insights From America's HIV Epidemic Analysis Dashboard (AHEAD) National Database. *Cureus*, *16*(10).

[76] Ayo-Farai, O., Obianyo, C., Ezeamii, V., & Jordan, K. (2023). Spatial Distributions of Environmental Air Pollutants Around Dumpsters at Residential Apartment Buildings.

[77] Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., Babarinde, A. O., & Sodamade, O. T. (2023). Telemedicine in Health Care: A Review of Progress and Challenges in Africa. *Matrix Science Pharma*, *7*(4), 124-132.

[78] Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., Babarinde, A. O., & Sodamade, O. T. (2024). Digital Health Technologies in Chronic Disease Management: A Global Perspective. *International Journal of Research and Scientific Innovation*, *10*(12), 533-551.

[79] Ayo-Farai, O., Olaide, B. A., Maduka, C. P., & Okongwu, C. C. (2023). Engineering innovations in Healthcare: A Review of Developments in the USA. *Engineering Science & Technology Journal*, *4*(6), 381-400.

[80] Azubuike, C., Sule, A. K., Adepoju, P. A., Ikwuanusi, U. F., & Odionu, C. S. (2024). Enhancing Small and Medium-Sized Enterprises (SMEs) Growth through Digital Transformation and Process Optimization: Strategies for Sustained Success. *International Journal of Research and Scientific Innovation*, *11*(12), 890-900.

[81] Azubuike, C., Sule, A. K., Adepoju, P. A., Ikwuanusi, U. F., & Odionu, C. S. (2024). Integrating Saas Products in Higher Education: Challenges and Best Practices in Enterprise Architecture. *International Journal of Research and Scientific Innovation*, *11*(12), 948-957.

[82] Babarinde, A. O., Ayo-Farai, O., Maduka, C. P., Okongwu, C. C., & Sodamade, O. (2023). Data analytics in public health, A USA perspective: A review. *World Journal of Advanced Research and Reviews*, *20*(3), 211-224.

[83] Babarinde, A. O., Ayo-Farai, O., Maduka, C. P., Okongwu, C. C., Ogundairo, O., & Sodamade, O. (2023). Review of AI applications in Healthcare: Comparative insights from the USA and Africa. *International Medical Science Research Journal*, *3*(3), 92-107.

[84] Balogun, O. D., Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., Babarinde, A. O., & Sodamade, O. T. (2024). The Role of pharmacists in personalised medicine: a review of integrating pharmacogenomics into clinical practice. *International Medical Science Research Journal*, *4*(1), 19-36.

[85] Balogun, O. D., Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., Babarinde, A. O., & Sodamade, O. T. (2023). Innovations in drug delivery systems: A review of the pharmacist's role in enhancing efficacy and patient compliance.

[86] Balogun, O. D., Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., Babarinde, A. O., & Sodamade, O. T. (2023). Integrating AI into health informatics for enhanced public health in Africa: a comprehensive review. *International Medical Science Research Journal*, *3*(3), 127-144.

[87] Bello, S., Wada, I., Ige, O., Chianumba, E., & Adebayo, S. (2024). AI-driven predictive maintenance and optimization of renewable energy systems for enhanced operational efficiency and longevity. *International Journal of Science and Research Archive*, *13*(1).

[88] Bidemi, A. I., Oyindamola, F. O., Odum, I., Stanley, O. E., Atta, J. A., Olatomide, A. M., ... & Helen, O. O. (2021). Challenges Facing Menstruating Adolescents: A Reproductive Health Approach. *Journal of Adolescent Health*, *68*(5), 1-10.

[89] Boumezbeur, I., & Zarour, K. (2022). Privacy-preserving and access control for sharing electronic health record using blockchain technology. Acta Informatica Pragensia, 11(1), 105-122.

[90] Chigboh, V. M., Zouo, S. J. C., & Olamijuwon, J. (2024). Health data analytics for precision medicine: A review of current practices and future directions. *International Medical Science Research Journal, 4*(11), 973–984. https://www.fepbl.com/index.php/imsrj/article/view/1732

[91] Chigboh, V. M., Zouo, S. J. C., & Olamijuwon, J. (2024). Predictive analytics in emergency healthcare systems: A conceptual framework for reducing response times and improving patient care. *World Journal of Advanced Pharmaceutical and Medical Research, 7*(2), 119–127. https://zealjournals.com/wjapmr/content/predictive-analytics-emergency-healthcare-systems-conceptual-framework-reducing-response

[92] Chintoh, G. A., Segun-Falade, O. D., Odionu, C. S., & Ekeh, A. H. (2024). Legal and ethical challenges in AI governance: A conceptual approach to developing ethical compliance models in the U.S. *International Journal of Social Science Exceptional Research*, *3*(1), 103-109. https://doi.org/10.54660/IJSSER.2024.3.1.103-109

[93] Chintoh, G. A., Segun-Falade, O. D., Odionu, C. S., & Ekeh, A. H. (2025). Cross-jurisdictional data privacy compliance in the U.S.: Developing a new model for managing AI data across state and federal laws. *Gulf Journal of Advanced Business Research*, *3*(2), 537-548. https://doi.org/10.51594/gjabr.v3i2.96

[94] Chintoh, G. A., Segun-Falade, O. D., Odionu, C. S., & Ekeh, A. H. (2025). The role of AI in U.S. consumer privacy: Developing new concepts for CCPA and GLBA compliance in smart services. *Gulf Journal of Advanced Business Research*, *3*(2), 549-560. https://doi.org/10.51594/gjabr.v3i2.97

[95] Chintoh, G. A., Segun-Falade, O. D., Odionu, C. S., & Ekeh, A. H. (2024). Developing a compliance model for AI in U.S. privacy regulations.

[96] Chintoh, G. A., Segun-Falade, O. D., Odionu, C. S., & Ekeh, A. H. (2024). Proposing a Data Privacy Impact Assessment (DPIA) model for AI projects under U.S. privacy regulations. *International Journal of Social Science Exceptional Research*, *3*(1), 95-102. https://doi.org/10.54660/IJSSER.2024.3.1.95-102

[97] Chintoh, G. A., Segun-Falade, O. D., Odionu, C. S., & Ekeh, A. H. (2024). Developing a Compliance Model for AI-Driven Financial Services: Navigating CCPA and GLBA Regulations.

[98] Chintoh, G. A., Segun-Falade, O. D., Odionu, C. S., & Ekeh, A. H. (2024). International Journal of Social Science Exceptional Research.

[99] Chukwurah, N., Abieba, O. A., Ayanbode, N., Ajayi, O. O., & Ifesinachi, A. (2024). Inclusive Cybersecurity Practices in AI-Enhanced Telecommunications: A Conceptual Framework.

[100] Dirlikov, E. (2021). Rapid scale-up of an antiretroviral therapy program before and during the COVID-19 pandemic—nine states, Nigeria, March 31, 2019–September 30, 2020. *MMWR. Morbidity and Mortality Weekly Report*, *70*.

[101] Dirlikov, E., Jahun, I., Odafe, S. F., Obinna, O., Onyenuobi, C., Ifunanya, M., ... & Swaminathan, M. (2021). Section navigation rapid scale-up of an antiretroviral therapy program before and during the COVID-19 pandemic-nine states, Nigeria, March 31, 2019-September 30, 2020.

[102] Edoh, N. L., Chigboh, V. M., Zouo, S. J. C., & Olamijuwon, J. (2024). Improving healthcare decision-making with predictive analytics: A conceptual approach to patient risk assessment and care optimization. *International Journal of Scholarly Research in Medicine and Dentistry, 3*(2), 1–10. https://srrjournals.com/ijsrmd/sites/default/files/IJSRMD-2024-0034.pdf

[103] Edoh, N. L., Chigboh, V. M., Zouo, S. J. C., & Olamijuwon, J. (2024). The role of data analytics in reducing healthcare disparities: A review of predictive models for health equity. *International Journal of Management & Entrepreneurship Research, 6*(11), 3819–3829. https://www.fepbl.com/index.php/ijmer/article/view/1721

[104] Edwards, Q., Ayo-Farai, O., Uwumiro, F. E., Komolafe, B., Chibuzor, O. E., Agu, I., ... & NWUKE, H. O. (2025). Decade-Long Trends in Hospitalization, Outcomes, and Emergency Department Visits for Inflammatory Bowel Diseases in the United States, 2010 to 2020. *Cureus*, *17*(1).

[105] Ekeh, A. H., Apeh, C. E., Odionu, C. S., & Austin-Gabriel, B. (2025). Automating Legal Compliance and Contract Management: Advances in Data Analytics for Risk Assessment, Regulatory Adherence, and Negotiation Optimization.

[106] Ekeh, A. H., Apeh, C. E., Odionu, C. S., & Austin-Gabriel, B. (2025). Data analytics and machine learning for gender-based violence prevention: A framework for policy design and intervention strategies. *Gulf Journal of Advance Business Research*, *3*(2), 323-347.

[107] Ekeh, A. H., Apeh, C. E., Odionu, C. S., & Austin-Gabriel, B. (2025). Leveraging machine learning for environmental policy innovation: Advances in Data Analytics to address urban and ecological challenges. *Gulf Journal of Advance Business Research*, *3*(2), 456-482.

[108] Ekeh, A. H., Apeh, C. E., Odionu, C. S., & Austin-Gabriel, B. (2025). Advanced Data Warehousing and Predictive Analytics for Economic Insights: A Holistic Framework for Stock Market Trends and GDP Analysis.

[109] Ezeamii, V. C., Gupta, J., Ayo-Farai, O., Savarese, M., & Adhikari, A. (2024). Assessment of VOCs and Molds Using CDC/NIOSH developed tools in Hurricane Ian affected Homes.

[110] Ezeamii, V. C., Ofochukwu, V. C., Iheagwara, C., Asibu, T., Ayo-Farai, O., Gebeyehu, Y. H., ... & Okobi, O. E. (2024). COVID-19 Vaccination Rates and Predictors of Uptake Among Adults With Coronary Heart Disease: Insight From the 2022 National Health Interview Survey. *Cureus*, *16*(1).

[111] Ezeamii, V. C., Ofochukwu, V. C., Iheagwara, C., Asibu, T., Ayo-Farai, O., Gebeyehu, Y. H., ... & Okobi, O. E. (2024). COVID-19 Vaccination Rates and Predictors of Uptake Among Adults With Coronary Heart Disease: Insight From the 2022 National Health Interview Survey. *Cureus*, *16*(1).

[112] Ezeamii, V., Adhikari, A., Caldwell, K. E., Ayo-Farai, O., Obiyano, C., & Kalu, K. A. (2023, November). Skin itching, eye irritations, and respiratory symptoms among swimming pool users and nearby residents in relation to stationary airborne chlorine gas exposure levels. In *APHA 2023 Annual Meeting and Expo*. APHA.

[113] Ezeamii, V., Ayo-Farai, O., Obianyo, C., Tasby, A., & Yin, J. (2024). A Preliminary Study on the Impact of Temperature and Other Environmental Factors on VOCs in Office Environment.

[114] Ezeamii, V., Jordan, K., Ayo-Farai, O., Obiyano, C., Kalu, K., & Soo, J. C. (2023). Dirunal and seasonal variations of atmospheric chlorine near swimming pools and overall surface microbial activity in surroundings.

[115] Fagbule, O. F., Amafah, J. O., Sarumi, A. T., Ibitoye, O. O., Jakpor, P. E., & Oluwafemi, A. M. (2023). Sugar-Sweetened Beverage Tax: A Crucial Component of a Multisectoral Approach to Combating Non-Communicable Diseases in Nigeria. *Nigerian Journal of Medicine*, *32*(5), 461-466.

[116] Fasipe, O.J. & Ogunboye, I., (2024). Elucidating and unravelling the novel antidepressant mechanism of action for atypical antipsychotics: repurposing the atypical antipsychotics for more comprehensive therapeutic usage. RPS Pharmacy and Pharmacology Reports, 3(3), p. rqae017. Available at: https://doi.org/10.1093/rpsppr/rqae017

[117] Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*, *24*(1), 2582-2595.

[118] Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). Security compliance and its implication for cybersecurity. *World Journal of Advanced Research and Reviews*, *24*(01), 2105-2121.

[119] Gbadegesin, J. O., Adekanmi, A. J., Akinmoladun, J. A., & Adelodun, A. M. (2022). Determination of Fetal gestational age in singleton pregnancies: Accuracy of ultrasonographic placenta thickness and volume at a Nigerian tertiary Hospital. *African Journal of Biomedical Research*, *25*(2), 113-119.

[120] Hackl, W., Hoerbst, A., & Ammenwerth, E. (2011). "why the hell do we need electronic health records?". Methods of Information in Medicine, 50(01), 53-61. https://doi.org/10.3414/me10-02-0020

[121] Hoffman, S. (2016). Electronic health records and medical big data.. https://doi.org/10.1017/9781316711149

[122] Hussain, N. Y., Austin-Gabriel, B., Adepoju, P. A., & Afolabi, A. I., 2024. AI and Predictive Modeling for Pharmaceutical Supply Chain Optimization and Market Analysis. International Journal of Engineering Research and Development, 20(12), pp.191-197.

[123] Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., Adepoju, P. A., and Afolabi, A. I., 2023. Generative AI advances for data-driven insights in IoT, cloud technologies, and big data challenges. Open Access Research Journal of Multidisciplinary Studies, 06(01), pp.051-059.

[124] Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I., 2021. AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. Open Access Research Journal of Science and Technology, 02(02), pp.006-015. https://doi.org/10.53022/oarjst.2021.2.2.0059

[125] Ibeh, A.I., Oso, O.B., Alli, O.I., & Babarinde, A.O. (2025) 'Scaling healthcare startups in emerging markets: A platform strategy for growth and impact', International Journal of Advanced Multidisciplinary Research and Studies, 5(1), pp. 838-854. Available at: http://www.multiresearchjournal.com/

[126] Ige, A. B., Adepoju, P. A., Akinade, A. O., & Afolabi, A. I. (2025). Machine Learning in Industrial Applications: An In-Depth Review and Future Directions.

[127] Ige, A. B., Akinade, A. O., Adepoju, P. A., & Afolabi, A. I. (2025). Reviewing the Impact of 5G Technology on Healthcare in African Nations. *International Journal of Research and Innovation in Social Science*, *9*(1), 1472-1484.

[128] Ige, A. B., Austin-Gabriel, B., Hussain, N. Y., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I., 2022. Developing multimodal AI systems for comprehensive threat detection and geospatial risk mitigation. Open Access Research Journal of Science and Technology, 06(01), pp.093-101. https://doi.org/10.53022/oarjst.2022.6.1.0063

[129] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., & Afolabi, A. I. (2024). Advancing Predictive Analytics Models for Supply Chain Optimization in Global Trade Systems. *International Journal of Applied Research in Social Sciences. https://doi. org/10.51594/ijarss. v6i12*. (1769)

[130] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews, 2*(1), 074–086. https://doi.org/10.30574/msarr.2021.2.1.0032

[131] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2023). Advancing machine learning frameworks for customer retention and propensity modeling in ecommerce platforms. *GSC Adv Res Rev*, *14*(2), 17.

[132] Ikwuanusi, U. F., Adepoju, P. A., & Odionu, C. S. (2023). Advancing ethical AI practices to solve data privacy issues in library systems. International Journal of Multidisciplinary Research Updates, 6(1), 033-044. https://doi.org/10.53430/ijmru.2023.6.1.0063

[133] Ikwuanusi, U. F., Adepoju, P. A., & Odionu, C. S. (2023). AI-driven solutions for personalized knowledge dissemination and inclusive library user experiences. International Journal of Engineering Research Updates, 4(2), 052-062. https://doi.org/10.53430/ijeru.2023.4.2.0023

[134] Ikwuanusi, U. F., Adepoju, P. A., & Odionu, C. S. (2023). Developing predictive analytics frameworks to optimize collection development in modern libraries. International Journal of Scientific Research Updates, 5(2), 116–128. https://doi.org/10.53430/ijsru.2023.5.2.0038

[135] Jahun, I., Dirlikov, E., Odafe, S., Yakubu, A., Boyd, A. T., Bachanas, P., ... & CDC Nigeria ART Surge Team. (2021). Ensuring optimal community HIV testing services in Nigeria using an enhanced community case-finding package (ECCP), October 2019–March 2020: acceleration to HIV epidemic control. *HIV/AIDS-Research and Palliative Care*, 839-850.

[136] Jahun, I., Said, I., El-Imam, I., Ehoche, A., Dalhatu, I., Yakubu, A., ... & Swaminathan, M. (2021). Optimizing community linkage to care and antiretroviral therapy Initiation: Lessons from the Nigeria HIV/AIDS Indicator and Impact Survey (NAIIS) and their adaptation in Nigeria ART Surge. *PLoS One*, *16*(9), e0257476.

[137] Kelvin-Agwu, M. C., Adelodun, M. O., Igwama, G. T., & Anyanwu, E. C. (2024): Enhancing Biomedical Engineering Education: Incorporating Practical Training in Equipment Installation and Maintenance.

[138] Kelvin-Agwu, M. C., Adelodun, M. O., Igwama, G. T., & Anyanwu, E. C. (2024): The Impact of Regular Maintenance on the Longevity and Performance of Radiology Equipment.

[139] Kelvin-Agwu, M. C., Adelodun, M. O., Igwama, G. T., & Anyanwu, E. C. (2024). Strategies for optimizing the management of medical equipment in large healthcare institutions. *Strategies*, *20*(9), 162-170.

[140] Kelvin-Agwu, M. C., Adelodun, M. O., Igwama, G. T., & Anyanwu, E. C. (2024). Advancements in biomedical device implants: A comprehensive review of current technologies. *Int. J. Front. Med. Surg. Res*, *6*, 19-28.

[141] Kelvin-Agwu, M. C., Adelodun, M. O., Igwama, G. T., & Anyanwu, E. C. (2024). Integrating biomedical engineering with open-source telehealth platforms: enhancing remote patient monitoring in global healthcare systems. *International Medical Science Research Journal*, *4*(9).

[142] Kelvin-Agwu, M. C., Adelodun, M. O., Igwama, G. T., & Anyanwu, E. C. (2024). The role of biomedical engineers in enhancing patient care through efficient equipment management. *International Journal Of Frontiers in Medicine and Surgery Research*, *6*(1), 11-18.

[143] Kelvin-Agwu, M. C., Adelodun, M. O., Igwama, G. T., & Anyanwu, E. C. (2024). Innovative approaches to the maintenance and repair of biomedical devices in resource-limited settings.

[144] Kruse, C., Goswamy, R., Raval, Y., & Marawi, S. (2016). Challenges and opportunities of big data in health care: a systematic review. Jmir Medical Informatics, 4(4), e38. https://doi.org/10.2196/medinform.5359

[145] Majebi, N. L., Adelodun, M. O., & Anyanwu, E. C. (2024). *Community-based interventions to prevent child abuse and neglect: A policy perspective*. *International Journal of Engineering Inventions, 13*(9), 367–374.

[146] Majebi, N. L., Adelodun, M. O., & Anyanwu, E. C. (2024). *Early childhood trauma and behavioral disorders: The role of healthcare access in breaking the cycle*. *Comprehensive Research and Reviews in Science and Technology, 2*(1), 080–090.

[147] Majebi, N. L., Adelodun, M. O., & Anyanwu, E. C. (2024). *Integrating trauma-informed practices in US educational systems: Addressing behavioral challenges in underserved communities*. *Comprehensive Research and Reviews in Science and Technology, 2*(1), 070–079.

[148] Majebi, N. L., Adelodun, M. O., & Anyanwu, E. C. (2024). *Maternal mortality and healthcare disparities: Addressing systemic inequities in underserved communities*. *International Journal of Engineering Inventions, 13*(9), 375–385.

[149] Majebi, N. L., Drakeford, O. M., Adelodun, M. O., & Anyanwu, E. C. (2023). *Leveraging digital health tools to improve early detection and management of developmental disorders in children*. *World Journal of Advanced Science and Technology, 4*(1), 025–032.

[150] Matthew, A., Opia, F. N., Matthew, K. A., Kumolu, A. F., & Matthew, T. F. (2021). Cancer Care Management in the COVID-19 Era: Challenges and adaptations in the global south. *Cancer*, *2*(6).

[151] Matthew, K. A., Akinwale, F. M., Opia, F. N., & Adenike, A. (2021). The Relationship between oral Contraceptive Use, Mammographic Breast Density, and Breast Cancer Risk.

[152] Matthew, K. A., Getz, K. R., Jeon, M. S., Luo, C., Luo, J., & Toriola, A. T. (2024). Associations of Vitamins and Related Cofactor Metabolites with Mammographic Breast Density in Premenopausal Women. *The Journal of Nutrition*, *154*(2), 424-434.

[153] Matthew, K. A., Nwaogelenya, F., & Opia, M. (2024). Conceptual review on the importance of data visualization tools for effective research communication. *International Journal Of Engineering Research and Development*, *20*(11), 1259-1268. https://ijerd.com/paper/vol20-issue11/201112591268.pdf

[154] Nnagha, E. M., Ademola Matthew, K., Izevbizua, E. A., Uwishema, O., Nazir, A., & Wellington, J. (2023). Tackling sickle cell crisis in Nigeria: the need for newer therapeutic solutions in sickle cell crisis management–short communication. *Annals of Medicine and Surgery*, *85*(5), 2282-2286.

[155] Nwaonumah, E., Riggins, A., Azu, E., Ayo-Farai, O., Chopak-Foss, J., Cowan, L., & Adhikari, A. (2023). A Refreshing Change: Safeguarding Mothers and Children from PFAS Exposure.

[156] Obianyo, C., Tasby, A., Ayo-Farai, O., Ezeamii, V., & Yin, J. (2024). Impact of Indoor Plants on Particulate Matter in Office Environments.

[157] Oddie-Okeke, C. C., Ayo-Farai, O., Iheagwara, C., Bolaji, O. O., Iyun, O. B., Zaynieva, S., & Okobi, O. E. (2024). Analyzing HIV Pre-exposure Prophylaxis and Viral Suppression Disparities: Insights From America's HIV Epidemic Analysis Dashboard (AHEAD) National Database. *Cureus*, *16*(8).

[158] Odionu, C. S., Adepoju, P. A., Ikwuanusi, U. F., Azubuike, C., & Sule, A. K. (2024). The impact of agile methodologies on IT service management: A study of ITIL framework implementation in banking. Engineering Science & Technology Journal, 5(12), 3297-3310. https://doi.org/10.51594/estj.v5i12.1786

[159] Odionu, C. S., Adepoju, P. A., Ikwuanusi, U. F., Azubuike, C., & Sule, A. K. (2024). Strategic implementation of business process improvement: A roadmap for digital banking success. International Journal of Engineering Research and Development, 20(12), 399-406. Retrieved from http://www.ijerd.com

[160] Odionu, C. S., Adepoju, P. A., Ikwuanusi, U. F., Azubuike, C., & Sule, A. K. (2024). The role of enterprise architecture in enhancing digital integration and security in higher education. International Journal of Engineering Research and Development, 20(12), 392-398. Retrieved from http://www.ijerd.com

[161] Odionu, C. S., Adepoju, P. A., Ikwuanusi, U. F., Azubuike, C., & Sule, A. K. (2024). The evolution of IT business analysis in the banking industry: Key strategies for success. International Journal of Multidisciplinary Research Updates, 8(2), 143-151. https://doi.org/10.53430/ijmru.2024.8.2.0066

[162] Odionu, C. S., Adepoju, P. A., Ikwuanusi, U. F., Azubuike, C., & Sule, A. K. (2025). The role of BPM tools in achieving digital transformation. International Journal of Research and Scientific Innovation (IJRSI), 11(12), 791. https://doi.org/10.51244/IJRSI.2024.11120071

[163] Ogbeta, C.P., Mbata, A.O. & Udemezue, K.K., 2025. Technology and regulatory compliance in pharmaceutical practices: Transforming healthcare delivery through data-driven solutions. International Journal of Research and Innovation in Social Science (IJRISS), 9(1), pp.1139-1144. DOI: https://dx.doi.org/10.47772/IJRISS.2025.9010095.

[164] Ogbeta, C.P., Mbata, A.O., & Katas, K.U., 2021. Innovative strategies in community and clinical pharmacy leadership: Advances in healthcare accessibility, patient-centered care, and environmental stewardship. Open Access Research Journal of Science and Technology, 2(2), pp.16-22. DOI: https://doi.org/10.53022/oarjst.2021.2.2.0046.

[165] Ogbeta, C.P., Mbata, A.O., & Katas, K.U., 2022. Advances in expanding access to mental health and public health services: Integrated approaches to address underserved populations. World Journal of Advanced Science and Technology, 2(2), pp.58-65. DOI: https://doi.org/10.53346/wjast.2022.2.2.0044.

[166] Ogbeta, C.P., Mbata, A.O., & Katas, K.U., 2025. Developing drug formularies and advocating for biotechnology growth: Pioneering healthcare innovation in emerging economies. International Journal of Multidisciplinary Research and Growth Evaluation, 6(1), pp.20-25. DOI: https://doi.org/10.54660/.IJMRGE.2025.6.1.20-25.

[167] Ogbeta, C.P., Mbata, A.O., Udemezue, K.K. & Kassem, R.G., 2023. Advancements in pharmaceutical quality control and clinical research coordination: Bridging gaps in global healthcare standards. IRE Journals, 7(3), pp.678-688. Available at: https://www.irejournals.com [Accessed 9 Feb. 2025].

[168] Ogugua, J. O., Anyanwu, E. C., Olorunsogo, T., Maduka, C. P., & Ayo-Farai, O. (2024). Ethics and strategy in vaccination: A review of public health policies and practices. *International Journal of Science and Research Archive*, *11*(1), 883-895.

[169] Ogunboye, I., Adebayo, I.P.S., Anioke, S.C., Egwuatu, E.C., Ajala, C.F. and Awuah, S.B. (2023) 'Enhancing Nigeria's health surveillance system: A data-driven approach to epidemic preparedness and response', World Journal of Advanced Research and Reviews, 20(1). Available at: https://doi.org/10.30574/wjarr.2023.20.1.2078.

[170] Ogunboye, I., Momah, R., Myla, A., Davis, A. and Adebayo, S. (2024) 'HIV screening uptake and disparities across socio-demographic characteristics among Mississippi adults: Behavioral Risk Factor Surveillance System (BRFSS), 2022', HPHR, 88. Available at: https://doi.org/10.54111/0001/JJJJ3.

[171] Ogunboye, I., Zhang, Z. & Hollins, A., (2024). The predictive socio-demographic factors for HIV testing among the adult population in Mississippi. HPHR, 88. Available at: https://doi.org/10.54111/0001/JJJJ1.

[172] Ogundairo, O., Ayo-Farai, O., Maduka, C. P., Okongwu, C. C., Babarinde, A. O., & Sodamade, O. T. (2023). Review on MALDI mass spectrometry and its application in clinical research. *International Medical Science Research Journal*, *3*(3), 108-126.

[173] Ogundairo, O., Ayo-Farai, O., Maduka, C. P., Okongwu, C. C., Babarinde, A. O., & Sodamade, O. T. (2024). Review on MALDI Imaging for Direct Tissue Imaging and its Application in Pharmaceutical Research. *International Journal of Research and Scientific Innovation*, *10*(12), 130-141.

[174] Ogundairo, O., Ayo-Farai, O., Maduka, C. P., Okongwu, C. C., Babarinde, A. O., & Sodamade, O. (2023). Review On Protein Footprinting As A Tool In Structural Biology. *Science Heritage Journal (GWS)*, *7*(2), 83-90.

[175] Ohalete, N. C., Ayo-Farai, O., Olorunsogo, T. O., Maduka, P., & Olorunsogo, T. (2024). AI-Driven Environmental Health Disease Modeling: A Review of Techniques and Their Impact on Public Health in the USA And African Contexts. *International Medical Science Research Journal*, *4*(1), 51-73.

[176] Ohalete, N. C., Ayo-Farai, O., Onwumere, C., & Paschal, C. (2024). Navier-stokes equations in biomedical engineering: A critical review of their use in medical device development in the USA and Africa.

[177] Ohalete, N. C., Ayo-Farai, O., Onwumere, C., Maduka, C. P., & Olorunsogo, T. O. (2024). Functional data analysis in health informatics: A comparative review of developments and applications in the USA and Africa.

[178] Okhawere, K. E., Grauer, R., Saini, I., Joel, I. T., Beksac, A. T., Ayo-Farai, O., ... & Badani, K. K. (2024). Factors associated with surgical refusal and non-surgical candidacy in stage 1 kidney cancer: a National Cancer Database (NCDB) analysis. *The Canadian Journal of Urology*, *31*(5), 11993.

[179] Okobi, O. E., Ayo-Farai, O., Tran, M., Ibeneme, C., Ihezie, C. O., Ezie, O. B., ... & Tran, M. H. (2024). The Impact of Infectious Diseases on Psychiatric Disorders: A Systematic Review. *Cureus*, *16*(8).

[180] Okon, R., Zouo, S. J. C., & Sobowale, A. (2024). Navigating complex mergers: A blueprint for strategic integration in emerging markets. *World Journal of Advanced Research and Reviews, 24*(2), 2378–2390. https://wjarr.com/content/navigating-complex-mergers-blueprint-strategic-integration-emerging-markets

[181] Okoro, Y. O., Ayo-Farai, O., Maduka, C. P., Okongwu, C. C., & Sodamade, O. T. (2024). The Role of technology in enhancing mental health advocacy: a systematic review. *International Journal of Applied Research in Social Sciences*, *6*(1), 37-50.

[182] Okoro, Y. O., Ayo-Farai, O., Maduka, C. P., Okongwu, C. C., & Sodamade, O. T. (2024). A review of health misinformation on digital platforms: challenges and countermeasures. *International journal of applied research in social sciences*, *6*(1), 23-36.

[183] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premise integrations.

[184] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2024). Frameworks for ethical data governance in machine learning: Privacy, fairness, and business optimization.

[185] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.3.2.0086

[186] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises integrations. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.3.1.0076

[187] Olamijuwon, J., & Zouo, S. J. C. (2024). The impact of health analytics on reducing healthcare costs in aging populations: A review. *International Journal of Management & Entrepreneurship Research*. https://www.fepbl.com/index.php/ijmer/article/view/1690

[188] Olorunsogo, T. O., Balogun, O. D., Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., & Onwumere, C. (2024). Mental health and social media in the US: A review: Investigating the potential links between online platforms and mental well-being among different age groups. *World Journal of Advanced Research and Reviews*, *21*(1), 321-334.

[189] Olorunsogo, T. O., Balogun, O. D., Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., & Onwumere, C. (2024). Bioinformatics and personalized medicine in the US: A comprehensive review: Scrutinizing the advancements in genomics and their potential to revolutionize healthcare delivery.

[190] Olorunsogo, T. O., Balogun, O. D., Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., & Onwumere, C. (2024). Reviewing the evolution of US telemedicine post-pandemic by analyzing its growth, acceptability, and challenges in remote healthcare delivery during Global Health Crises. *World Journal of Biology Pharmacy and Health Sciences*, *17*(1), 075-090.

[191] Olowe, K. J., Edoh, N. L., Zouo, S. J. C., & Olamijuwon, J. (2024). Review of predictive modeling and machine learning applications in financial service analysis. *Computer Science & IT Research Journal, 5*(11), 2609–2626. https://fepbl.com/index.php/csitrj/article/view/1731

[192] Olowe, K. J., Edoh, N. L., Zouo, S. J. C., & Olamijuwon, J. (2024). Conceptual frameworks and innovative biostatistical approaches for advancing public health research initiatives. *International Journal of Scholarly Research in Medicine and Dentistry, 3*(2), 11–21. https://srrjournals.com/ijsrmd/content/conceptual-frameworks-and-innovative-biostatistical-approaches-advancing-public-health

[193] Olowe, K. J., Edoh, N. L., Zouo, S. J. C., & Olamijuwon, J. (2024). Comprehensive review of advanced data analytics techniques for enhancing clinical research outcomes. *International Journal of Scholarly Research in Biology and Pharmacy, 5*(1), 8–17. https://srrjournals.com/ijsrbp/content/comprehensive-review-advanced-data-analytics-techniques-enhancing-clinical-research-outcomes

[194] Olowe, K. J., Edoh, N. L., Zouo, S. J. C., & Olamijuwon, J. (2024). Comprehensive review of logistic regression techniques in predicting health outcomes and trends. *World Journal of Advanced Pharmaceutical and Life Sciences, 7*(2), 16–26. https://zealjournals.com/wjapls/sites/default/files/WJAPLS-2024-0039.pdf

[195] Olowe, K. J., Edoh, N. L., Zouo, S. J. C., & Olamijuwon, J. (2024). Theoretical perspectives on biostatistics and its multifaceted applications in global health studies. *International Journal of Applied Research in Social Sciences, 6*(11), 2791–2806. https://www.fepbl.com/index.php/ijarss/article/view/1726

[196] Olowe, K. J., Edoh, N. L., Zouo, S. J. C., & Olamijuwon, J. (2024). Conceptual review on the importance of data visualization tools for effective research communication. *International Journal of Engineering Research and Development, 20*(11), 1259–1268. https://ijerd.com/paper/vol20-issue11/201112591268.pdf

[197] Oluwole, O., Haggarty, N., Ikenyei, U., Tinuoye, O., Honora, A., & Issakah, M. (2023). Strategies and tools for electronic health records and physician workflow alignment: a scoping review protocol.. https://doi.org/10.1101/2023.12.27.23300587

[198] Opia, F. N., & Matthew, K. A. (2025): Empowering Unrepresented Populations Through Inclusive Policy Frameworks In Global Health Initiatives.

[199] Opia, F. N., Matthew, K. A., & Matthew, T. F. (2022). Leveraging Algorithmic and Machine Learning Technologies for Breast Cancer Management in Sub-Saharan Africa.

[200] Oshodi, A. N., Adelodun, M. O., Anyanwu, E. C., & Majebi, N. L. (2024). *Combining parental controls and educational programs to enhance child safety online effectively*. *International Journal of Applied Research in Social Sciences, 6*(9), 2293-2314.

[201] Oso, O.B., Alli, O.I., Babarinde, A.O. & Ibeh, A.I. (2025) 'Advanced financial modeling in healthcare investments: A framework for optimizing sustainability and impact', Gulf Journal of Advance Business Research, 3(2), pp. 561-589. Available at: https://doi.org/10.51594/gjabr.v3i2.98

[202] Oso, O.B., Alli, O.I., Babarinde, A.O., & Ibeh, A.I. (2025) 'Impact-driven healthcare investments: A conceptual framework for deploying capital and technology in frontier markets', International Journal of Multidisciplinary Research and Growth Evaluation, 6(1), pp. 1702-1720. Available at: https://doi.org/10.54660/IJMRGE.2025.6.1.1702-1720

[203] Oso, O.B., Alli, O.I., Babarinde, A.O., & Ibeh, A.I. (2025) 'Private equity and value creation in healthcare: A strategic model for emerging markets', International Journal of Medical and All Body Health Research, 6(1), pp. 55-73. Available at: https://doi.org/10.54660/IJMBHR.2025.6.1.55-73

[204] Otieno, O. and Loice, H. (2019). Security and privacy determinants for a secured cloud-based electronic health record system. International Journal of Engineering Applied Sciences and Technology, 4(3), 35-47. https://doi.org/10.33564/ijeast.2019.v04i03.005

[205] Patel, R. D., Abramowitz, C., Shamsian, E., Okhawere, K. E., Deluxe, A., Ayo-Farai, O., ... & Badani, K. K. (2022, June). Is YouTube a good resource for patients to better understand kidney cancer?. In *Urologic Oncology: Seminars and Original Investigations* (Vol. 40, No. 6, pp. 275-e19). Elsevier.

[206] Patel, R. D., Abramowitz, C., Shamsian, E., Okhawere, K. E., Deluxe, A., & Ayo-Farai, O. & Badani, KK (2022, June). Is YouTube a good resource for patients to better understand kidney cancer. In *Urologic Oncology: Seminars and Original Investigations* (Vol. 40, No. 6, pp. 275-e19).

[207] Provenzano, M., Cillara, N., Curcio, F., Pisu, M., González, C., & Herrera, M. (2024). Electronic health record adoption and its effects on healthcare staff: a qualitative study of well-being and workplace stress. International Journal of Environmental Research and Public Health, 21(11), 1430. https://doi.org/10.3390/ijerph21111430

[208] Rahman, M. S., Khalil, I., Mahawaga Arachchige, P. C., Bouras, A., & Yi, X. (2019, July). A novel architecture for tamper proof electronic health record management system using blockchain wrapper. In Proceedings of the 2019 ACM international symposium on blockchain and secure critical infrastructure (pp. 97-105).

[209] Rezaeibagha, F., Win, K., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Information Management Journal, 44(3), 23-38. https://doi.org/10.1177/183335831504400304

[210] Sharma, V., Gupta, A., Hasan, N. U., Shabaz, M., & Ofori, I. (2022). [Retracted] Blockchain in Secure Healthcare Systems: State of the Art, Limitations, and Future Directions. Security and Communication Networks, 2022(1), 9697545.

[211] Shittu, R. A., Ehidiamen, A. J., Ojo, O. O., Zouo, S. J. C., Olamijuwon, J., Omowole, B. M., & Olufemi-Phillips, A. Q. (2024). The role of business intelligence tools in improving healthcare patient outcomes and operations. *World Journal of Advanced Research and Reviews, 24*(2), 1039–1060. https://wjarr.com/sites/default/files/WJARR-2024-3414.pdf

[212] Sule, A. K., Adepoju, P. A., Ikwuanusi, U. F., Azubuike, C., & Odionu, C. S. (2024). Optimizing customer service in telecommunications: Leveraging technology and data for enhanced user experience. International Journal of Engineering Research and Development, 20(12), 407-415. Retrieved from http://www.ijerd.com

[213] Temedie-Asogwa, T., Atta, J. A., Al Zoubi, M. A. M., & Amafah, J. (2024). Economic Impact of Early Detection Programs for Cardiovascular Disease.

[214] Tertulino, R., Antunes, N., & Morais, A. (2023). Privacy in electronic health records: a systematic mapping study. Journal of Public Health, 32(3), 435-454. https://doi.org/10.1007/s10389-022-01795-z

[215] Tertulino, R., Ivaki, N., & Morais, A. (2024). Design a software reference architecture to enhance privacy and security in electronic health records.. https://doi.org/10.21203/rs.3.rs-4006291/v1

[216] Uwumiro, F. E., Ayo-Farai, O., Uduigwome, E. O., Nwebonyi, S., Amadi, E. S., Faniyi, O. A., ... & Aguchibe, R. (2024). Burden of In-Hospital Admissions and Outcomes of Thoracic Outlet Compression Syndrome in the United States From 2010 to 2021. *Cureus*, *16*(10).

[217] Uwumiro, F., Nebuwa, C., Nwevo, C. O., Okpujie, V., Osemwota, O., Obi, E. S., ... & Ekeh, C. N. (2023). Cardiovascular Event Predictors in Hospitalized Chronic Kidney Disease (CKD) Patients: A Nationwide Inpatient Sample Analysis. *Cureus*, *15*(10).

[218] Zouo, S. J. C., & Olamijuwon, J. (2024). Financial data analytics in healthcare: A review of approaches to improve efficiency and reduce costs. *Open Access Research Journal of Science and Technology, 12*(2), 10–19. http://oarjst.com/content/financial-data-analytics-healthcare-review-approaches-improve-efficiency-and-reduce-costs

[219] Zouo, S. J. C., & Olamijuwon, J. (2024). Machine learning in budget forecasting for corporate finance: A conceptual model for improving financial planning. *Open Access Research Journal of Multidisciplinary Studies, 8*(2), 32–40. https://oarjpublication.com/journals/oarjms/content/machine-learning-budget-forecasting-corporate-finance-conceptual-model-improving-financial

[220] Zouo, S. J. C., & Olamijuwon, J. (2024). The intersection of financial modeling and public health: A conceptual exploration of cost-effective healthcare delivery. *Finance & Accounting Research Journal, 6*(11), 2108–2119. https://www.fepbl.com/index.php/farj/article/view/1699