International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-13, Issue-6, November 2025
DOI: https://doi.org/10.55524/ijircst.2025.13.6.13
Article ID IJIRE-1415, Pages 121-131
www.ijircst.org

AI-Based Anomaly Detection and Legal-Risk Assessment Framework for Protecting Electronic Health Records

Gnanesh Methari[1] and Abdullah Mazharuddin Khaja[2]

[1] Department of Information Technology (Cybersecurity), Franklin University, Columbus, United States
[2] Department of Computer Science, Governors State University, University Park, Illinois, United States

Correspondence should be addressed to Gnanesh Methari; Metharignanesh770@gmail.com

Received: 1 November 2025 Revised: 16 November 2025 Accepted: 29 November 2025

Copyright © 2025 Made Gnanesh Methari et al. This is an open-access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT- Electronic Health Records (EHRs) have become common in the health systems of many countries across the globe. They assist physicians and hospitals in storing and exchanging patient data within a short period of time. The rise of EHRs usage, however, has also raised the chances of data breaches and cyberattacks. Hackers create a threat to the healthcare data, and insiders may abuse it as well. Conventional security systems do not necessarily work in identifying these threats. Due to this reason, there has been increased usage of artificial intelligence (AI) to detect abnormal or suspicious activity in the EHR systems. Most of the literature concentrates on the level of AI detection of anomalies and lacks legal and regulatory risks. This review unites the studies on the topic of AI-based anomaly detection and the laws related to healthcare data protection. It points out major differences between technical security and legal compliance. A basic structure combining AI detection and legal-risk assessment is also suggested in the paper because it would enhance data protection and decrease legal risk.

KEYWORDS- EHRs, Anomaly detection, Cybersecurity, Healthcare, Legal risk, Data privacy, AI.

I. INTRODUCTION

The global healthcare systems are experiencing significant digital transformation [1]. Previously, most of the patient information was kept on paper. These were paper records that took time to access and were hard to share between hospitals and physicians [2]. In the modern world, most healthcare organizations are shifting to digital systems. The use of Electronic Health Records (EHRs) is one of the most significant changes. EHRs enable the storage, updating, and sharing of the patient data electronically. This assists the doctors in making prompt choices and enhances care quality. There are numerous advantages of using EHRs. Patient information can be accessed within a short period of time by the healthcare staff. It is possible to minimize medical errors [3]. One can share information between departments and even among countries. EHRs are also useful in research, reporting and healthcare planning. Due to these benefits, governments and healthcare providers are putting every effort to encourage the establishment of digital health systems. However, this digital transformation also introduces some new issues. When patient information is kept electronically it is vulnerable to cyberattacks. Healthcare data is very valuable to hackers since it is personal, medical, and financial information [4]. Digital records are accessible remotely as opposed to the paper record that is accessible only in the office. This enlarges the amount of attack points. With the growing interconnection of healthcare systems, the chances of breaches of data also rise. The wide application of the EHR systems worldwide demonstrates the magnitude of this problem. Figure 1 shows the adoption rate of Electronic Health Records in the selected countries in the world in terms of percentage. As the figure indicates, in most of the developed healthcare systems EHR adoption is very high. To mention a few, in the United States, the adoption rates are approximately 95 per cent, South Korea is 97 per cent, Australia is 93 per cent and Norway is 90 per cent. The level of adoption is also high at the European Union at about 86%. These statistics suggest that EHRs have become the norm in record keeping in most of the regions.

Simultaneously, Figure 1 also indicates cross-country differences. Developed countries are highly adopting the rate, but certain developing areas are still within the initial phase. As an example, India has an adoption rate of about 25 and South Africa is nearer to 60. Such variations indicate that EHR systems are growing in the world at varying rates. With this growing adoption in the developing countries, the amount of digital health data will expand even more.

The numerical data presented in the below Figure 1 effectively indicates that the use of EHRs is not restricted to the several countries any longer. Instead, it is a global trend. It implies that the EHR-related security problems are also international. One health system can have a data breach that impacts millions of patients [5]. It also has the potential to undermine confidence in digital healthcare solutions. Hence, the security of EHR systems is not purely a technical problem. It is an international healthcare issue.

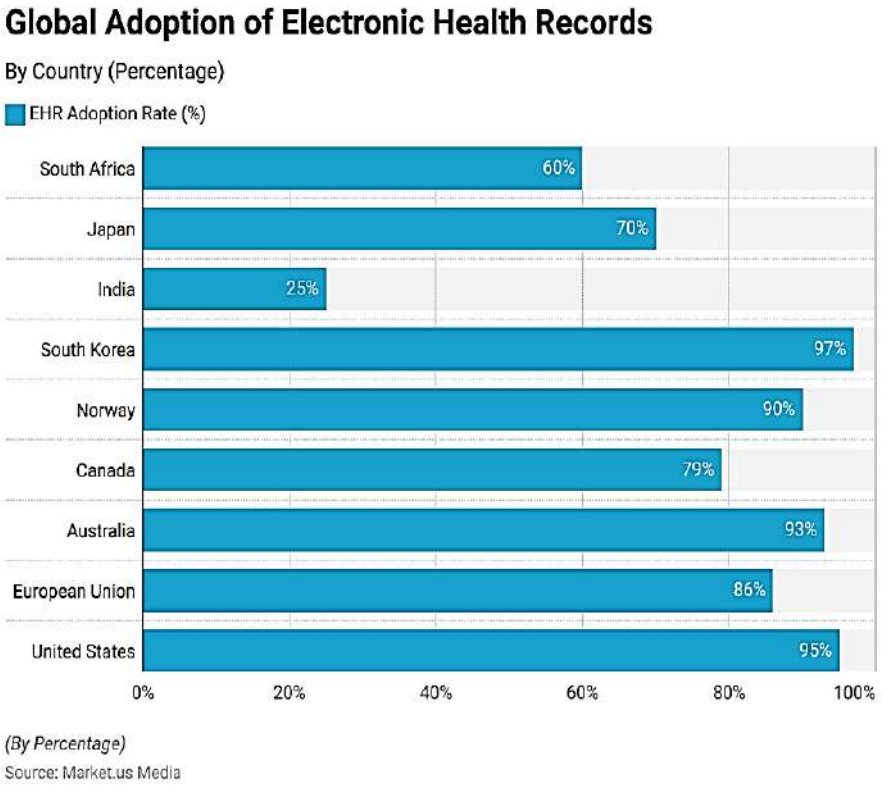


Figure 1: Global Adoption of EHR

The conventional security systems are usually regulation based. They base it on set policies to identify perceived dangers. Although they are effective in blocking certain attacks, they are not as effective in detecting new threats or concealed ones [6]. The healthcare setting is dynamic and complicated. The data are accessed by users in their time and place. Owing to this, abnormal or maladaptive behavior might not necessarily be predictable.

Here, it is crucial to note artificial intelligence (AI). The behavior of a normal system can be learnt by AI-based systems. Then they can identify an abnormal activity that could show the existence of security threat. This is referred to as anomaly detection [7]. AI-based anomaly detection particularly comes in handy in the medical field since it can process massive and complex data sets. It is also able to adapt to new forms of attack.

In summary, the Electronic Health Records global shift has changed the manner in which healthcare is provided. Although EHRs enhance the quality of care and its efficiency, they also elevate cybersecurity risks. Figure 1 demonstrates high adoption rates which prove that EHR protection is a prevalent issue across the world. It is observed that this scenario describes the necessity of smart, dynamic security measures, including AI-based anomaly detection, to safeguard patient data and facilitate the safe digital healthcare framework.

II. REVIEW SCOPE, TYPE, AND METHODOLOGICAL APPROACH

A. Type of Review

This research is based on integrative narrative review. This form of review is appropriate in cases where studies in other disciplines should be synthesized. This paper synthesizes the work of artificial intelligence, cybersecurity, healthcare, and law. The systematic review was not selected due to the goal not to address a single specific question. Rather, the aim is to get to know a larger problem and build new knowledge.

Integrative narrative review permits discussing theories, methods, and concepts in a flexible manner [8]. It also facilitates comparison across study which utilizes various approaches and types of data. Such a method can be used to tell patterns, gaps, and connections between technical and legal research. It is particularly beneficial in the case of new subjects where studies are in their advancement. These reasons make this method of review appropriate to the objective of implementing the AI-based anomaly detection and legal-risk evaluation on EHR protection.

B. Literature Sources

This review was based on literature retrieved through popular academic databases. These are IEEE Xplore, Scopus, Web of Science, PubMed and Google Scholar. The choice of these sources was informed by the fact that they discuss studies in computer science, medicine, and legal studies.

The relevant studies were found with a variety of keywords. They comprised the expressions connected with electronic health records, anomaly detection, artificial intelligence, healthcare cybersecurity, data privacy, and compliance with the law. Current and extensive studies were taken into consideration to avoid one-sidedness in existing and background research. Also, policy reports and regulatory documents were examined to facilitate the legal discussion.

C. Inclusion Criteria

Studies were selected based on clear criteria in this review. Peer-reviewed journal articles, conference papers and

authoritative reports were provided only. The studies had to center on either of the following areas: EHR security, AI-based anomaly detection, healthcare data breaches, or legal and regulatory risks.

Articles that were not related to healthcare systems were left out. The studies that had a limited scope in terms of security or legal matters were not taken into consideration as well. Preference was made to the research that was published within the past decade because during this time, the sphere of digital healthcare and AI technologies experienced rapid growth.

D. AI and Legal-Risk Synthesis

In this review, the primary focus is the combination of AI-based anomaly and legal-risk measurements. Most of the current literature addresses these issues individually. Technical research is usually interested in the accuracy of detection, whereas legal research is interested in compliance and punishment. This review makes these two areas unite.

This paper tries to identify how events that resulted in security can have legal consequences by synthesizing technical and legal literature. Such combined attention assists in the creation of a system that could assist healthcare organizations to enhance both data protection and litigation mitigation.

III. ELECTRONIC HEALTH RECORDS: LEGAL AND SECURITY ISSUES

A. Nature and Sensitivity of EHR Data

EHRs are records which include patient details. Such information is produced and maintained during the lifetime of an individual. It contains numerous forms of information. Typical ones include personal information, i.e. name, date of birth, address. Medical history, diagnoses, test results, prescriptions as well as treatment plans are also stored in EHRs. They also contain the insurance information and the billing information in most cases [9].

EHRs are very sensitive to this large amount of data. Medical data is sensitive and confidential. Patients hope that this information will remain confidential. It is not easy to alter health records if they are stolen unlike in other forms of data [10]. Leaked medical condition or diagnosis may impact on one throughout his or her life. This is what renders the healthcare data more valuable than most other kinds of digital information.

There are numerous users of EHR systems. Patient data must be accessible to the doctors, nurses, lab technicians, pharmacists, and the administrative staff [11]. In other instances, other people like insurers or researchers may have little access too. This is because healthcare delivery requires these multiple access points, which also pose a security risk. Every part of access can be used to be abused or attacked.

EHRs can be accessed anywhere. Contemporary systems are usually cloud-based and networked. The information may be retrieved across the various sub-units and places [12]. Even though this enhances efficiency, it exposes one to cyber threats. When the access controls are weak or not properly controlled, the attackers can take advantage of the weak controls.

Attackers find healthcare data very valuable because of several reasons. It is saleable in the black markets. One can use it to commit identity theft, insurance fraud, or blackmail [13]. In ransomware attacks, hackers prevent access to EHR systems and reimburse them. Since hospitals are dependent on these systems, they are usually forced to pay. These reasons give healthcare organizations an excellent target of cybercriminals.

B. Cybersecurity Risks and Data breach trends.

The number and impact of healthcare data breaches have grown in recent years. Along with the increasing digitization of healthcare systems, the systems also become more susceptible to cyber threats [14]. The breach of data may have numerous reasons. There are those that are because of attacks by outside people and those that are because of the internal acts or breakdown of the system. These threats, combined, pose a complex security environment.

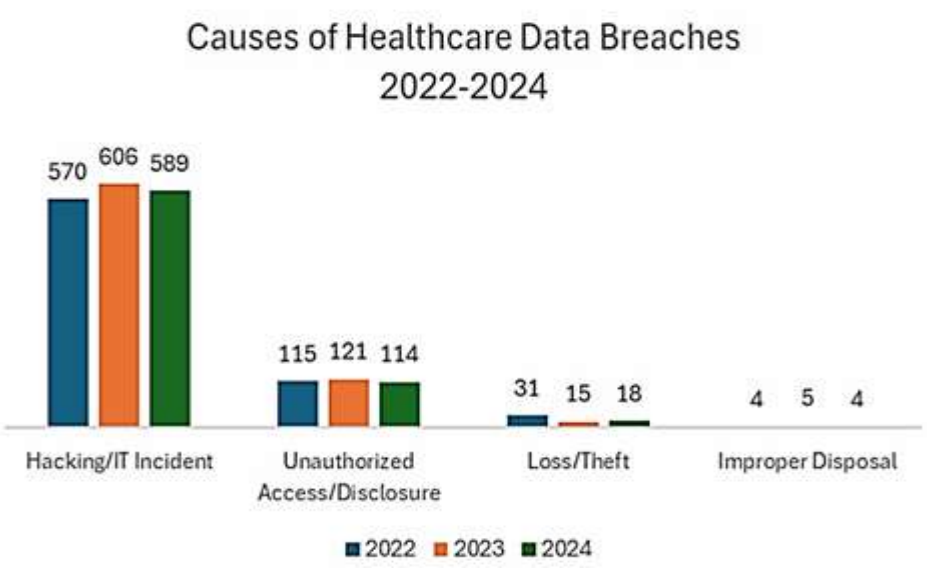
One of the leading sources of healthcare data breaches includes external cyberattacks. Such attacks are hacking, malware, and ransomware. Hackers can use weak passwords, software that has expired, or software that has been misconfigured [15]. After gaining access to the system, they may steal bulk patient information or cause havoc to the operations of the hospital. Ransomware attacks are particularly harmful in that they can halt access to important systems.

There are also the threats of internal threats. They can include unauthorized access to data by the employees or misuse of it [16]. In other instances, breaches may occur because of human error, which includes sending the data to the wrong recipient or the loss of devices holding patient information. These actions might not be harmful, but they still can lead to severe data exposure.

The magnitude of these threats is shown in recent breach statistics. In the below Figure 2 demonstrates the main causes of healthcare data breaches in 2022-2024. As the figure indicates, the highest percentage of breaches is always caused by hacking and IT related incidents that impact millions of patient records annually. Comparatively, internal misuse and unintentional disclosures are small yet significant parts.

The prevalence of cyber-related incidents in Figure 2 makes a crucial point. With conventional security systems, there is a tendency of detecting known threats based on predefined rules. Most contemporary attacks are, however, not predictable. Attackers always adapt to evade the detection. Consequently, new or concealed threats might go undetected by rule-based systems.

This is a trend that favors the more adaptive security solutions. Anomaly detection is aimed at detecting abnormal behavior instead of signature attacks. Anomaly detection systems can identify suspicious activities real-time by understanding what the normal system activity should behave like.



(Source: HIPAA Journal)

Figure 2: Causes of Healthcare Data Breaches 2022-24

The trends exhibited in Figure 2 are thus a good reason to abandon the use of conventional security tools and use the practices of AI.

C. Legal and Regulatory Implications of EHR Breach.

The consequences of an EHR data breach are not confined to technical harm. Healthcare organizations are also exposed to severe legal and regulatory repercussions [17]. Most nations have stringent legislation which safeguards patient information. Such legislation enforces organizations to observe good security practices and report breaches on a timely basis.

Penalties in law courts may be harsh. Failure to secure patient information by healthcare providers may result in huge financial penalties [18]. They might also be obliged to pay damages to the injured patients. In other instances, organizations may be audited or monitored over a long period of time by regulators. These are expensive and time-consuming processes.

Failure to comply also hurts trust. The inability to safeguard the information of patients may undermine the trust of the patients in healthcare providers [19]. This may cause reputational damage and losing patients. This can also impact on revenue and partnerships of the private healthcare organizations. Even the state healthcare systems can experience social pressure and criticism when they experience significant breach.

All these trends point to the fact that technical failures in EHR security are, often, directly converted into legal and regulatory risks, and that are the reasons why a comprehensive security and compliance approach should be implemented.

IV. AI-BASED ANOMALY DETECTION FOR EHR SECURITY

A. Anomaly Detection as a Concept in Healthcare Systems.

Digital data is produced in large volumes in healthcare systems daily. The information is provided by EHRs, user access logs, medical devices, and network activity [20]. With this type of complex system, security threats cannot be defined at all. This is why standard rule-based methods of security may prove to be insufficient.

Anomaly detection is a method of security that deals with the detection of abnormal behavior. Rather than searching for previous attack patterns, it searches for activities that are not normal system behavior [21]. The basic idea is simple. First, the system is taught normal activity appearance. It is followed by the observation of new activity and then flags something that seems abnormal. Such abnormal events can signify security threats, misuse or system errors.

The anomaly detection is particularly handy in healthcare settings. The health care systems are dynamic. The EHRs are accessed by users in a time-variable manner and location. The access patterns may vary based on the emergency, shift, or the needs of patients. Due to this reason, hard coded security policies can give numerous false alarms or can fail to detect actual threats. These changes can be accommodated by anomaly detecting systems with time.

Some of the abnormalities in EHR systems include abnormal login hours, access to a significant number of patient records, or access to records numerous times without an apparent medical necessity [22]. Such behaviors can imply misuse of their insiders or external attacks. Anomaly detection systems may be used to prevent severe data breaches by identifying them beforehand.

The approaches to anomaly detection may be classified into various categories depending on the mode of data analysis. Figure 3 below gives a taxonomy of anomaly detection methods, with some of the most popular methods in the literature represented. These are statistical, machine learning, information-theoretic as well as streaming-based techniques. All categories possess a variety of strengths and weaknesses. There are methods that are easy and quick and there are those that are not very complicated but are more precise.

B. Machine Learning-Based Approaches

Altogether, anomaly detection offers a dynamic and versatile method of EHR system monitoring. It has some obvious benefits when compared with conventional security mechanisms, particularly in more complicated healthcare settings where the threat continues to evolve. Anomaly detection in EHR systems is popularly applied using machine learning. These approaches enable systems to infer patterns using data rather than using rules. This renders them more adaptive and applicable to complicated settings in healthcare.

A typical method is that of classification. In the classical-based methods, the system is trained with labelled data. It is indicated that the data is either normal or abnormal [23]. After the training, the model can categorize the events in these categories. Decision tree, support vector machine and random forest are common types of classifiers. Such approaches work well in cases where there is quality labelled data. Nonetheless, labelled attack data is also not always available in the context of healthcare. This can reduce performance.

Clustering is another useful method. The clustering techniques take related data and cluster them without labeling. Two clusters, normal behavior and anomalies are typically large and small, respectively [24]. K-means and DBSCAN algorithms are commonly employed. Clustering is effective where the patterns of attacks are not known. The selection of the right number of clusters may be challenging though. When the data is noisy it may also decrease performance.

Distance-based algorithms observe anomalies by the measure of the distance between a source of data and others. In case a data point is remote to most normal points, it is considered as abnormal [25]. Such techniques are easy to comprehend and simple. Nevertheless, they do not scale appropriately with large EHR datasets.

Density-based techniques emphasize regions with high concentrations of data points. Normal behavior tends to be concentrated in areas of high density whereas anomalies tend to be spread sparsely [26]. These techniques can process sophisticated patterns as compared to simple distance-based techniques. Nevertheless, they might not be able to handle data of extreme dimensions.

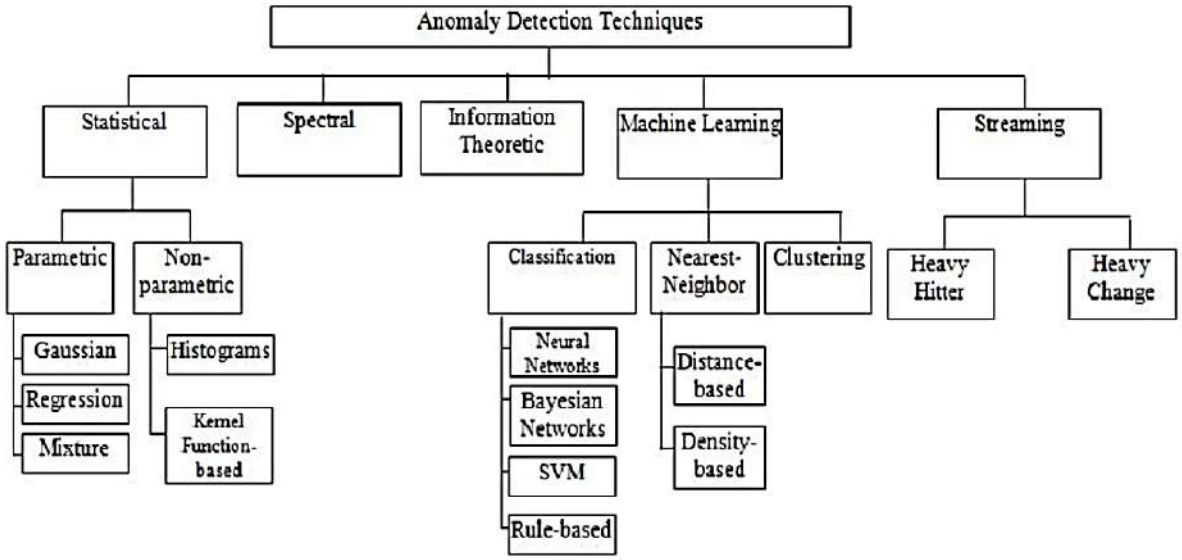


Figure 3: Anomaly Detection Techniques

As illustrated in Figure 3, the key types of anomaly detection methods in security systems are clearly outlined. The figure classifies such techniques according to the analysis of data and the detection of abnormal behavior. This taxonomy makes the reader aware of the broad horizon of the methods that are talked about in literature.

The first level splits anomaly detection into four major groups recognized by the figure. These include information-theoretic approaches, statistics techniques, machine learning approaches, and streaming techniques. Both groups are the alternative definitions of what is deemed as normal behavior. Statistical techniques are based on probability models and past averages. They assume that normal behavior is distributed in a steady manner. Any sharp variation that is not consistent with this trend is indicated as an anomaly. These techniques are easy and quick but have problems coping with complicated or dynamic EHR settings. Machine learning techniques occupy the most significant portion of the figure. These are classification, clustering, distance based and density-based methods. These approaches acquire patterns using data as indicated in Figure 3. They are more adaptable than statistical solutions and may adjust to the changing user behavior within the EHR systems.

The information-theoretic approaches emphasize variations in the information content (Entropy). The abrupt surges of uncertainty can signal the abnormal workings of the system. Such are practical in identifying minor alterations but are not as frequently applied in healthcare. Lastly, streaming-based methods are meant to analyze real time data. They constantly track incoming information streams, including access logs of EHR. This renders them appropriate in real-time threat detection and amplifies the computation requirements.

In general, Figure 3 can be used to understand the relationship between various anomaly detection methods. It also describes the reason why machine learning and deep learning techniques have dominated the current EHR

security studies. This fact justifies the shift in the old-fashioned approaches to new AI-based methodologies covered in this review.

C. Deep Learning and Hybrid Models

Nowadays, deep learning techniques have been paid close attention to the detection of anomalies in EHRs. These models are quite appropriate with large and complex datasets. They have the capability to automatically discover intricate patterns without designing features.

An autoencoder is one of the most common deep learning models. Autoencoders are trained to reduce normal data and restore them [27]. Reconstruction errors are high when abnormal data is passed through the model. This is a mistake which is used to identify anomalies. Autoencoders are useful in high-dimensional EHR data. They are particularly effective where there is the unavailability of labelled attack data. Nonetheless, they need great volumes of data and powerful computers.

RNNs and LSTM models can also be applied with time-based data. The EHR access logs tend to be time-based [28]. The LSTM models can record asset-long-term dependencies in the user behavior. They are willing to give an example; it can look at the abnormal access patterns or abrupt modifications of the usage patterns. These models are effective in the detection of insider threats. Training them, however, is complex and time consuming.

Deep learning models, although very accurate, have a significant weakness. This is low explainability. These models can be called black boxes [29]. One cannot easily clarify how a particular event was considered abnormal. This is a health care problem. Decisions are often demanded by legal and regulatory structures to be clear. Lack of transparency may decrease trust and legal acceptance.

To resolve this problem, there is an increase in the use of hybrid models. The hybrid methods are combinations of techniques. One can see an example where a system is based on deep learning detection and rule-based explanation [30]. There are other hybrid models that involve the use of machine learning and statistical techniques. These models are designed to compromise on accuracy and interpretability.

Hybrid models are particularly helpful in the EHR settings. They can detect more complicated threats and also deliver comprehensible outputs. They are however more complex to design and maintain. They also need to be intimately integrated amongst the various system components. In general, deep learning and hybrid models are the most developed solutions to EHR anomaly detection. Although they are very powerful in terms of performance, the problems of explainability, cost and complexity are also critical problems.

D. Comparison of AI Techniques for Anomaly Detection in EHR Systems

To combine the advantages and disadvantages of the reviewed methods, Table 1 puts significant AI-based anomaly detection methods against each other regarding their data requirements, performance, and applicability to EHR settings.

Table 1: Comparison of AI Techniques for Anomaly Detection in EHR Systems

AI Technique	Data Type	Strengths	Limitations	Suitability for EHRs
Statistical	Structured	Simple, fast	Low accuracy	Limited
Machine Learning	Semi-structured	Scalable	Needs labels	Moderate
Deep Learning	Complex	High accuracy	Low explainability	High
Hybrid Models	Mixed	Balanced performance	High complexity	Very High

This table shows obvious trade-offs between techniques. The statistical methods are simple to apply and do not provide accuracy. Machine learning models enhance flexibility and, in most cases, require labeled data. Deep learning algorithm is very accurate and lacks transparency. Hybrid models provide optimal balance but entail increased complexity of the system. This comparison shows synthesis over literature and informed choice of methods to be used, regarding the real-world EHR security systems.

V. LAW-RISK ASSESSMENT IN AI-BASED HEALTHCARE SECURITY

A. Healthcare Data Management Legal Risk

There are numerous legal risks that healthcare organizations encounter in dealing with electronic health records (EHRs). Data breach may result in breach of privacy laws, either national or international. Examples of such laws and regulations are laws like HIPAA in the United States, GDPR in the European Union and other local data protection laws [31]. Legal risks are associated with the inability of organizations to ensure the safety of patient data or to report breaches in a timely manner. Such risks are not confined to fines only. Even the organizations can be sued by the affected patients or partners. Another major impact is reputational damage [32]. Patients can lose confidence in health care providers, and this can influence the utilization of the hospitals and financial results. Moreover, recurrent violations may open the way to long-term regulatory investigation. To prevent these dangers, healthcare providers are expected to have good data security practices.

As Figure 2 above has indicated, cyber-attacks take precedence in healthcare data breaches. This tendency makes healthcare providers more exposed to regulation. The greater the frequency and the severity of the cyberattacks is, the greater the legal consequences are. Therefore, contemporary healthcare operations need to know and control these risks

B. AI Accountability

Artificial intelligence (AI) application in healthcare security presents new legal implications. AI systems are automatically based on making decisions like flagging abnormal behaviors in EHR systems [33]. As much as

these decisions have the potential of enhancing security, they cause concerns of accountability. If an AI system cannot identify an attack, or is inaccurate in identifying legitimate activity, who is to blame? Compliance is ultimately the responsibility of healthcare organizations. They are unable to delegate the legal responsibility to AI systems and vendors fully [34]. This implies that organizations would have to put in place appropriate governance, monitoring, and auditing procedures. The AI models should be assessed, validated, and documented to meet the regulatory standards. AI decisions should be explainable and have transparency to be accepted legally and ethically. Low interpretability of black-box systems can pose a challenge to compliance, particularly where regulators would want to know how decisions made on patient data have been reached.

C. Compliance Gaps

Despite regulations and AI tools, there are usually compliance gaps in healthcare systems. Such gaps can be caused by the outdated security policies or the incomplete adoption of AI tools or the absence of staff training [35]. Certain organizations can adopt anomaly detection and not apply it to legal reporting practices. Others can only use technical security without even thinking of the regulation requirement.

There are severe consequences of compliance gaps. Although there is a likelihood of a breach being detected early, the result of breaching reporting rules can be fines or court proceedings. Likewise, documentation, auditing, or staff responsibility lapses may necessitate proving compliance. These loopholes indicate that it is necessary to use a comprehensive approach that integrates technical security, AI surveillance, and legal-risk management.

D. AI Security and Legal-Risk Assessment

Healthcare organizations need to combine AI-based security with legal-risk evaluation to mitigate the risks associated with legal liabilities. The detection of anomalies that are based on AI has the potential to minimize the technical vulnerabilities, as it detects suspicious patterns of access or activity [36]. Legal-risk assessment will make sure that such alerts are correctly understood and responded to in line with regulatory standards.

Such incorporation needs definite procedures. In case of an anomaly, the system should categorize the seriousness of the instance. The staff should review alerts with the assistance of personnel trained in cybersecurity and legal compliance [37]. The reporting standards ought to be in line with the local legislation and global standards. The records of all the steps used can assist in proving due diligence in situations where legal investigations may arise.

The framework also favors the process of continuous improvement. Both AI models and compliance procedures can be informed by the lessons learned on the identified anomalies. The policies can be revised to seal the loopholes and ensure fewer violations in the future and exposure to the law.

Overall, EHR breaches constitute the major legal risks that healthcare organizations encounter. Artificial intelligence systems enhance the detection of anomalies and raise ethical issues of accountability. Gaps in compliance may add to the effects of breaches in case they remain unaddressed. Regulatory exposure is more urgent than ever, as it relates to cyber-related incidents as illustrated in Figure 2.

Proactive strategy incorporates AI-based anomaly detection with systematic legal-risk evaluation. This will ensure that regulatory compliance does not stand alone with technical security measures. It also enables the organizations to respond swiftly, minimize legal reprimands and still preserve patient trust. To ensure future healthcare security approaches, AI and legal risk should not be viewed as separate issues, but rather as inseparable items.

VI. SMART AI-BASED FRAMEWORK OF ANOMALY DETECTION AND LEGAL-RISK ASSESSMENT

A. Need for integration

Modern healthcare cybersecurity research usually addresses technical and legal aspects independently. The majority of the studies are aimed at the refinement of the anomaly detection by the means of AI or at legal and regulatory compliance analysis. Although both are significant, there are only a few studies that relate the two areas. This division leads to the gap in the EHR security management. Technical systems can identify abnormal behaviour but healthcare organisations are rather unaware of the legal consequences of an incident. Likewise, legal frameworks offer regulations and punishments but hardly directly associate them with the technical monitoring data [38]. Such lack of connection may result in delays in reporting violations, compliance and amplified organisational risk.

Healthcare systems are not only complex in nature but require both data protection and legal compliance. An AI can notice the abnormal access to the patient records, e.g. Otherwise, the organisation might fail to react properly without a framework that reveals the legal meaning. The violation may go undetected, or unnecessary legal processes may be initiated. A combination of AI results and legal-risk assessment can be used to facilitate an assessment of anomalies on a technical and regulatory basis. This method will reduce confusion, enhanced response time, and enhanced overall protection of data.

B. AI-Outputs to Legal-Risk Scoring

AI-based anomaly detection is the first step in the proposed framework. The AI system is constantly scanned over EHR systems with the aim of identifying abnormal behaviour that may include abnormal times of logins, excess access to data, or abnormal patterns of access to patient records. After an anomaly is identified the system generates a risk score which is dependent on severity, frequency and possible impact.

These AI results are connected to a legal-risk scoring tool. Every identified anomaly is analyzed regarding applicable laws, including HIPAA, GDPR, or national healthcare data legislation [39]. The module has taken into account such aspects as the nature of the data concerned, the number of records, and the risk of patient damage. As an example, one log in by a known user can be of low risk legally whereas mass export of patient records would be of high risk. The combination of AI results with legal scoring enables healthcare organisations to place more emphasis

on incidents of both technical and regulatory importance. Organisational context is also explained in the framework. Various hospitals or clinics might have different reporting requirements, internal policies or patient population. The organisations can tailor their responses by feeding AI-generated anomalies into a legal-risk model. The risky incidents may activate immediate reporting to the regulators, legal teams, and management. Incidents of medium risk might entail in house investigation and mitigation. Anomalies with low risks can be recorded to track. This scoring process will make sure that legal obligation is fulfilled yet unnecessary measures are not taken.

C. Decision Support for Healthcare Organisations

In addition to scoring, the integrated framework offers decision support. The information is a combination of AI and legal-risk to formulate management actions. Some of the measures that could be proposed by the system include informing regulators, warn the patients or carry out internal audits. It is also capable of prescribing preventive actions, e.g. tightening controls on access or policy changes.

Decision support is required since in most cases, the staffs of healthcare might have so much work. Complex environments might also require human judgement which might not be capable of determining all the anomalies promptly [40]. The framework saves time on decision making since it gives practical recommendations, which makes the decisions consistent. It enhances interdepartmental communication as well. The same organized information regarding identified anomalies and their legal perspectives is provided to technical teams, legal officers and management.

The other benefit of integrated decision support is the capability to trace the trends over a period of time. The framework will be able to detect recurrent issues by comparing legal-risk evaluation with AI detection logs. As an illustration, frequent attempts to log into particular patient information can be regarded as insider threats. These patterns can be identified by the system, and early intervention and specific changes in the policy can be done. This preventive measure aids in minimizing future violations and court liability.

D. Advantages of an Integrated Framework.

There are some advantages to combining AI-based anomaly detection and legal-risk assessment. To begin with, it enhances relevance and accuracy. Only AI can identify abnormal behaviour, but not all anomalies will be of legal concern [41]. Taking the detection and scoring to the law, organisations are addressing the most important thing.

Second, it increases compliance and reporting. The framework also provides that high-risk incidents reported are done in accordance with the law. This minimizes fines, penalties and reputational losses. It also has good audit trails showing the proactive EHR security management. Third, the framework facilitates prioritisation of risks. There are thousands of anomalies that can be generated on a daily basis and human beings cannot manually test all the incidents. The scoring system enables prioritisation to be based on technical severity and the regulatory impact [42]. Cases with high priority are automatically escalated whereas low-priority cases are monitored. Lastly, integration promotes learning and constant improvement. The changes in AI models saw the introduction of new threats, and the legal modules were updated according to the change in regulations. New attack patterns, change in policies, and organisational changes can be accommodated in the framework. In the long run, it turns into a powerful instrument of ensuring safe and non-compliant EHR systems.

Conceptual Diagram (Placeholder)- The suggested framework will be depicted in a diagram where the flow will be shown between EHR system and organisational response. All functions are connected in a continuous process; every step is a different function. The feedback loops will also be featured in the diagram, and the new incidents that modify AI models and legal-risk rules will be highlighted. This graphical display emphasizes the incorporation and demonstrates how the framework works in reality.

Finally, the integrated framework responds to a severe healthcare cybersecurity gap. Connecting the technical monitoring with regulatory compliance, it links AI-based anomaly detection with legal-risk assessment. This solution will make sure that irregularities are assessed not only in relation to security but also in relation to legality. It assists in making decisions, prioritisation of incidents, enhancing reporting as well as augmenting overall protection of patient information. The framework is scalable, flexible and adaptable to new threats and evolving regulations. In this way, it is one of the main efforts to enhance EHR security within the contemporary healthcare infrastructure.

E. Ethical, Privacy and Governance

Patient data is very sensitive to healthcare organisations. Securing this information is not a technical problem but a moral one as well. Patient trust is one of the most crucial issues. The patients should be assured of the safety of their personal and medical data. Violation or abuse of data may seriously harm this trust. Failure to trust the system would make patients fail to give their information and this would be detrimental to healthcare results.

Other important aspects are transparency. The systems of AI-based anomaly detection may be complicated. Most sophisticated models, particularly deep learning are black boxes. They are able to issue red flags of suspicious activity without giving a reason [43]. This ambiguity can raise some ethical issues. Patients and healthcare personnel have a right to understand the nature of decision making. Regulators can also insist on the explanation of flagged events. Figure 3 presents a variety of techniques, which emphasizes the significance of explainability. Simple statistical procedures are not difficult to go through as well as the hybrid models are both precise and understandable. Performance and transparency should be put in balance through ethical oversight.

Data protection is mainly associated with governance. Organisations need to establish clear data access, use and sharing policies. These rules are enforced with the help of regular audits, risk assessment, and compliance checks [44]. Governance makes sure that systems of detecting anomalies are performed fairly and legally. It also instructs the staff on how to use and react to alerts. Well-developed governance structures make it less probable that abuse and

misuse will occur and promote the ability of organisations to satisfy the demands of the law.
The same can be applied to the development of AI in terms of ethical and privacy concerns. Bias, fairness, and accountability are some of the issues that developers need to take into consideration. The systems ought to be put through tests so that they do not discriminate some groups. Human experts should be able to review any automated decision making. Healthcare organisations can act responsibly and ethically by applying AI-based security through the combination of transparency, patient trust, and governance.

VII. CHALLENGES, LIMITATIONS, AND RESEARCH GAPS

In spite of the potential of AI-based anomaly detection, some challenges still exist. Information imbalance is one of the greatest problems. In healthcare, the majority of data reflects typical activity, whereas anomalies are few. Such unbalance renders it hard to develop the correct models. Models can overlook infrequent attacks or wrongly mark normal behavior as such. To counter these imbalances, researchers should devise techniques to deal with them, e.g., oversampling anomalies or synthetic data.
Legal uncertainty is another challenge. The legislations and regulations regarding healthcare data vary among nations [45]. There are strict rules and vague ones. There are several regulations that AI systems need to adhere to concurrently, and this is not always an easy task. In case of an anomaly, it is not always obvious how to react to it by law. Failure to manage compliance properly exposes organisations to punishment. This is one of the uncertainties that may slow down the implementation of AI in healthcare.
Another important limitation is the AI opacity. Numerous machine learning and deep learning schemes can be used without explicit descriptions [46]. Although they are good at identifying threats, it may be challenging to know why a system indicated that a record was a threat. Such absence of transparency complicates decision making, accountability and reporting to the regulators. It also brings ethical issues as the stakeholders might not believe in the decisions that they cannot decode.
Computational cost and complexity of the system are other weaknesses. The sophisticated models demand extensive data and processing power. These systems are costly to implement and maintain in hospitals. It is also difficult to integrate with the pre-existing EHR systems. Moreover, technical performance is the subject of many studies, and the practical implementation and human factors are frequently overlooked.
There is still a gap in research in a number of areas. Not many studies combine AI anomaly detection with legal-risk assessment on a more holistic level. The majority of work is devoted to the technical or legal accuracy respectively. Few studies on explainable AI approaches in healthcare have also been conducted. The hybrid solutions, cross-country law systems, and balance-seeking strategies in terms of accuracy, transparency, and cost require further research. Filling in these gaps will enable the healthcare organisations to embrace the AI-based security in a more secure and effective manner.

VIII. FUTURE RESEARCH DIRECTIONS

Anomaly detection and legal-risk assessment applied to EHR systems with the use of AI remains a developing field. There are numerous ways of how future research may be done. Among others, one of the directions is the enhancement of AI models explainability. The accuracy of deep learning and hybrid models is high in terms of detection, yet they are usually described as black boxes. Further research might be aimed at methods that can be used to give clear explanations to anomalies detected. This will assist the health care providers in learning about alerts and promote regulatory compliance.
The other research direction is to deal with limited or imbalanced data. In the healthcare industry, there is limited labelled attack data [47]. The machine learning techniques often require large datasets, and they may not be present. Creating techniques with effective working with small, semi-labeled, or synthetic data will enhance the usefulness of AI systems in clinical practice.
Another important field is integration with legal and regulatory frameworks. The future research must examine the possibility to directly connect AI detection systems to compliance monitoring, breach reporting, and risk mitigation [48]. This involves taking into account variation in laws in different regions and matching technical alerts and legal obligations.
Combinations of AI methods are likely to have an impact but require more development. Studies can be aimed at balancing accuracy, complexity and interpretability. Light and scalable hybrid systems that can operate in both large and small hospitals would be very handy.
Another priority is the ethical application of AI in healthcare. To overcome issues of bias in models, patient privacy, and responsible use of automated alerts must be tackled in future research. Ethics and standards would be useful in ensuring that AI systems do not harm patients unwillingly.
Lastly, there is real time monitoring and adaptive learning. Threats are also dynamic and EHR systems are dynamic. Such AI systems that are able to learn continuously and adapt to new behaviour patterns will be more effective when it comes to preventing breaches. Anomaly detecting and predictive analytics would also be a good combination to assist organisations to foresee risks before they can happen.
Altogether, the areas of future research are explainability, data scarcity, integrating regulations, fine-tuning hybrid models, ethics, and adaptive monitoring. These initiatives will enhance the security of EHR, as well as its compliance with legal and organisational demands.

IX. CONCLUSION

This review has explored how AI-based anomaly detection and legal-risk assessment can be used to safeguard Electronic Health Records. EHR systems have taken center stage in the contemporary healthcare and have enhanced efficiency, information exchange and patient care. Nevertheless, they also pose a high level of cybersecurity risks since they are widely used. Healthcare information is very sensitive and valuable and hence it is an easy target of external intruders as well as internal abuse.
The nature and sensitivity of EHR data were initially outlined in the paper. It emphasized numerous entry points,

the sophisticated nature of data, and the importance of healthcare data to attackers. The following review focused on cybersecurity threats and trends of breaches with the help of recent statistics. Figure 2 also depicted that the prevailing causes of breaches are hacking and IT incidents, thus the need to have proactive detection mechanisms.

Then, the review examined AI-based tools of anomaly detection. Machine learning, deep learning and hybrid models provide adaptive and flexible ways of detecting the unusual behaviour in EHR systems. These strategies were summarised in Figure 3 and Table 1 and their strengths and weaknesses and applicability to healthcare environments were identified. It was demonstrated that although AI techniques enhance detection, there are still issues especially in terms of explainability, data accessibility, and model complexity.

Legal and regulatory implications were also taken into consideration. Breaches not only jeopardize patient information, but also compromise compliance, and reputational damage, as well as potentially result in hefty fines. To respond promptly to incidents and stay within the healthcare regulations, the integration of AI detection and legal-risk assessment can be applied to assist organisations respond faster to incidents.

Lastly, the directions of future research were given. The most important problems are the creation of explainable AI models, the solution of data scarcity, refinement of hybrid solutions, technical and legal monitoring integration, ethical use of AI, and adaptive and real-time monitoring systems.

To conclude, the security of EHRs is a matter of both technical invention and legal knowledge. AI-driven anomaly detection suggests robust technologies to detect threats, yet they have to be consistent with regulations and ethical principles. Through the combination of AI techniques and legal-risk analysis, healthcare organisations will be able to enhance data security, minimize possible liability, and avoid losing the trust of patients. This review gives a basis to the future work and the significance of integrating both technical and legal approaches in protecting digital health information across the world.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Menon, A. K., X. Jiang, J. Kim, J. Vaidya, and L. Ohno-Machado, "Detecting inappropriate access to electronic health records using collaborative filtering," *Machine Learning*, vol. 95, no. 1, pp. 87–101, 2013. Available from: https://doi.org/10.1007/s10994-013-5376-1

[2] Bernardo, B. M. V., H. S. Mamede, J. M. P. Barroso, and V. M. P. D. dos Santos, "Data governance & quality management—Innovation and breakthroughs across different fields," *Journal of Innovation & Knowledge*, vol. 9, no. 4, p. 100598, 2024. Available from: https://doi.org/10.1016/j.jik.2024.100598

[3] Edozie, E., A. N. Shuaibu, B. O. Sadiq, and U. K. John, "Artificial intelligence advances in anomaly detection for telecom networks," *Artificial Intelligence Review*, vol. 58, no. 4, 2025. Available from: https://doi.org/10.1007/s10462-025-11108-x

[4] Diana, L., P. Dini, and D. Paolini, "Overview on intrusion detection systems for computer networking security," *Computers*, vol. 14, no. 3, p. 87, 2025. Available from: https://doi.org/10.3390/computers14030087

[5] Mennella, C., U. Maniscalco, G. D. Pietro, and M. Esposito, "Ethical and regulatory challenges of AI technologies in healthcare: A narrative review," *Heliyon*, vol. 10, no. 4, p. e26297, 2024. Available from: https://doi.org/10.1016/j.heliyon.2024.e26297

[6] Madan, R., N. Das, R. Patley, N. Nagpal, Y. Malik, and S. B. Math, "Consequences of medical negligence and litigations on health care providers – A narrative review," *Indian Journal of Psychiatry*, vol. 66, no. 4, pp. 317–325, 2024. Available from: https://doi.org/10.4103/indianjpsychiatry.indianjpsychiatry_799_23

[7] Jimma, B. L. and D. B. Enyew, "Barriers to the acceptance of electronic medical records from the perspective of physicians and nurses: A scoping review," *Informatics in Medicine Unlocked*, vol. 31, p. 100991, 2022. Available from: https://doi.org/10.1016/j.imu.2022.100991

[8] Xia, L., Z. Cao, and Y. Zhao, "Paradigm transformation of global health data regulation: Challenges in governance and human rights protection of cross-border data flows," *Risk Management and Healthcare Policy*, vol. 17, pp. 3291–3304, 2024. Available from: https://doi.org/10.2147/RMHP.S450082

[9] Ehrenstein, V., H. Kharrazi, H. Lehmann, and C. O. Taylor, "Obtaining data from electronic health records," Agency for Healthcare Research and Quality (US), 2020. Available from: https://www.ncbi.nlm.nih.gov/books/NBK551878/

[10] Sowmya, T. and E. A. M. Anita, "A comprehensive review of AI based intrusion detection system," *Measurement: Sensors*, vol. 28, p. 100827, 2023. Available from: https://doi.org/10.1016/j.measen.2023.100827

[11] Pool, J. K., S. Akhlaghpour, F. Fatehi, and A. B. Jones, "A systematic analysis of failures in protecting personal health data: A scoping review," *International Journal of Information Management*, vol. 74, p. 102719, 2024. Available from: https://www.sciencedirect.com/science/article/pii/S0268401223001007

[12] Inayat, U., M. Farzan, S. Mahmood, M. F. Zia, S. Hussain, and F. Pallonetto, "Insider threat mitigation: Systematic literature review," *Ain Shams Engineering Journal*, vol. 15, no. 12, p. 103068, 2024. Available from: https://doi.org/10.1016/j.asej.2024.103068

[13] Ondogan, A. G., M. Sargin, and K. Canoz, "Use of electronic medical records in the digital healthcare system and its role in communication and medical information sharing among healthcare professionals," *Informatics in Medicine Unlocked*, vol. 42, p. 101373, 2023. Available from: https://doi.org/10.1016/j.imu.2023.101373

[14] Sufi, F., "Addressing data scarcity in the medical domain: A GPT-based approach for synthetic data generation and feature extraction," *Information*, vol. 15, no. 5, p. 264, 2024. Available from: https://doi.org/10.3390/info15050264

[15] Novoa-Paradela, D., O. Fontenla-Romero, and B. Guijarro-Berdiñas, "A one-class classification method based on expanded non-convex hulls," *Information Fusion*, vol. 89, pp. 1–15, 2023. Available from: https://doi.org/10.1016/j.inffus.2022.07.023

[16] Bjerring, J. C., J. Mainz, and L. Munch, "Deep learning models and the limits of explainable artificial intelligence," *Asian Journal of Philosophy*, vol. 4, no. 1, 2025. Available from: https://doi.org/10.1007/s44204-024-00238-8

[17] Huang, Z., Z. Liang, S. Zhou, and S. Zhang, "An improved density-based spatial clustering of applications with noise algorithm with an adaptive parameter based on the sparrow search algorithm," *Algorithms*, vol. 18, no. 5, p. 273, 2025. Available from: https://doi.org/10.3390/a18050273

[18] Pinto, S. O. and V. A. Sobreiro, "Literature review: Anomaly detection approaches on digital business financial systems,"

Digital Business, vol. 2, no. 2, p. 100038, 2022. Available from: https://doi.org/10.1016/j.digbus.2022.100038

[19] Abdelwanis, M., M. C. E. Simsekler, A. F. Gabor, A. Sleptchenko, and M. Omar, "Artificial intelligence adoption challenges from healthcare providers' perspectives: A comprehensive review and future directions," *Safety Science*, vol. 193, p. 107028, 2025. Available from: https://doi.org/10.1016/j.ssci.2025.107028

[20] Muhammad Ishfaque, Q. Dai, N. ul Haq, K. Jadoon, S. M. Shahzad, and H. T. Janjuhah, "Use of recurrent neural network with long short-term memory for seepage prediction at Tarbela Dam, KP, Pakistan," *Energies*, vol. 15, no. 9, p. 3123, 2022. Available from: https://doi.org/10.3390/en15093123

[21] Yeo, L. H. and J. Banfield, "Human factors in electronic health records cybersecurity breach: An exploratory analysis," *Perspectives in Health Information Management*, vol. 19, 2022. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/

[22] Chimbo, B. and L. Motsi, "The effects of electronic health records on medical error reduction," *JMIR Medical Informatics*, vol. 12, p. e54572, 2024. Available from: https://doi.org/10.2196/54572

[23] Ayo, F. E., L. A. Ogundele, S. Olakunle, J. B. Awotunde, and F. A. Kasali, "A hybrid correlation-based deep learning model for email spam classification," *Decision Analytics Journal*, vol. 10, p. 100390, 2024. Available from: https://doi.org/10.1016/j.dajour.2023.100390

[24] Li, S., K. Surineni, and N. Prabhakaran, "Cyber-attacks on hospital systems: A narrative review," *American Journal of Geriatric Psychiatry: Open Science, Education, and Practice*, vol. 7, 2025. Available from: https://doi.org/10.1016/j.osep.2025.03.002

[25] Chen, S. and W. Guo, "Auto-encoders in deep learning—A review with new perspectives," *Mathematics*, vol. 11, no. 8, p. 1777, 2023. Available from: https://doi.org/10.3390/math11081777

[26] Mensah, N. K. *et al.*, "Health professionals' ethical, security, and patient safety concerns using digital health technologies," *Health Services Insights*, vol. 17, 2024. Available from: https://doi.org/10.1177/11786329241303379

[27] Barbaria, S. *et al.*, "Advancing compliance with HIPAA and GDPR in healthcare," *Healthcare*, vol. 13, no. 20, p. 2594, 2025. Available from: https://doi.org/10.3390/healthcare13202594

[28] Qian, H. *et al.*, "From black boxes to glass boxes: Explainable AI for trustworthy deepfake forensics," *Cryptography*, vol. 9, no. 4, p. 61, 2025. Available from: https://doi.org/10.3390/cryptography9040061

[29] Olukoya, O., "Assessing frameworks for eliciting privacy & security requirements," *Computers & Security*, vol. 117, p. 102697, 2022. Available from: https://doi.org/10.1016/j.cose.2022.102697

[30] Tariq, R. A. and P. B. Hackert, "Patient confidentiality," National Library of Medicine, 2023. Available from: https://www.ncbi.nlm.nih.gov/books/NBK519540/

[31] Singh, J. and D. Singh, "A comprehensive review of clustering techniques in artificial intelligence," *Advanced Engineering Informatics*, vol. 62, p. 102799, 2024. Available from: https://doi.org/10.1016/j.aei.2024.102799

[32] Wasylewicz, A. T. M. and A. M. J. W. Scheepers-Hoeks, "Clinical decision support systems," PubMed, 2018. Available from: https://www.ncbi.nlm.nih.gov/books/NBK543516/

[33] Chuma, K. G., "Legacy electronic health record systems as cybersecurity risks," *Global Security Health Science and Policy*, vol. 10, no. 1, 2025. Available from: https://doi.org/10.1080/23779497.2025.2532556

[34] HIPAA Journal, "What are the penalties for HIPAA violations?" 2024. Available from: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

[35] Vicoveanu, D. *et al.*, "Patient health record smart network challenges," *Sensors*, vol. 25, no. 12, p. 3710, 2025. Available from: https://doi.org/10.3390/s25123710

[36] Seh, A. H. *et al.*, "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, pp. 1–18, 2020. Available from: https://doi.org/10.3390/healthcare8020133

[37] Sukhera, J., "Narrative reviews: Flexible, rigorous, and practical," *Journal of Graduate Medical Education*, vol. 14, no. 4, pp. 414–417, 2022. Available from: https://doi.org/10.4300/jgme-d-22-00480.1

[38] Mohamed, N., "Artificial intelligence and machine learning in cybersecurity," *Knowledge and Information Systems*, vol. 67, pp. 6969–7055, 2025. Available from: https://doi.org/10.1007/s10115-025-02429-y

[39] Zeng, H. *et al.*, "AI-driven anomaly detection in smart city IoT networks," *Journal of Innovation & Knowledge*, vol. 9, no. 4, p. 100601, 2024. Available from: https://doi.org/10.1016/j.jik.2024.100601

[40] Conduah, A. K., S. Ofoe, and D. Siaw-Marfo, "Data privacy in healthcare," *Digital Health*, vol. 11, 2025. Available from: https://doi.org/10.1177/20552076251343959

[41] Sharma, A., S. Rani, and M. Shabaz, "A comprehensive review of explainable AI in cybersecurity," *ICT Express*, vol. 11, no. 6, 2025. Available from: https://doi.org/10.1016/j.icte.2025.10.004

[42] Koppel, R. and C. Kuziemsky, "Healthcare data are remarkably vulnerable to hacking," *Studies in Health Technology and Informatics*, vol. 257, pp. 218–222, 2019. Available from: https://pubmed.ncbi.nlm.nih.gov/30741199/

[43] Naik, N. *et al.*, "Legal and ethical consideration in artificial intelligence in healthcare," *Frontiers in Surgery*, vol. 9, p. 862322, 2022. Available from: https://doi.org/10.3389/fsurg.2022.862322

[44] Stoumpos, A. I., F. Kitsios, and M. A. Talias, "Digital transformation in healthcare," *International Journal of Environmental Research and Public Health*, vol. 20, no. 4, 2023. Available from: https://www.mdpi.com/1660-4601/20/4/3407

[45] Al-Dulaimy, A. *et al.*, "The computing continuum: From IoT to the cloud," *Internet of Things*, vol. 27, p. 101272, 2024. Available from: https://doi.org/10.1016/j.iot.2024.101272

[46] Garcia-Segura, L. A., "The role of artificial intelligence in preventing corporate crime," *Journal of Economic Criminology*, vol. 5, p. 100091, 2024. Available from: https://doi.org/10.1016/j.jeconc.2024.100091

[47] Okolie, S. A. *et al.*, "Anomaly detection in heterogeneous cybersecurity data," *Franklin Open*, vol. 13, p. 100426, 2025. Available from: https://doi.org/10.1016/j.fraope.2025.100426

[48] Lin, Y. and X. Li, "Back to the metrics: Exploration of distance metrics in anomaly detection," *Applied Sciences*, vol. 14, no. 16, p. 7016, 2024. Available from: https://doi.org/10.3390/app14167016