Developing trustworthy and ethically-based healthcare systems

Rami Ahmad
CET, American University in the Emirates, Dubai, United Arab Emirates

Received 18 May 2025
Revised 12 June 2025
Accepted 22 June 2025

Abstract

Purpose – This study proposes a practical, ethics-by-design framework that helps healthcare organizations safeguard patient privacy, comply with regulations, and retain clinical efficiency as they adopt cloud-enabled and AI-assisted digital health services.

Design/methodology/approach – A three-tier architecture is modelled. At the user layer, explicit, revocable consent tokens govern data sharing. At the clinical layer, Electronic Health-Record (EHR) workflows are reinforced with HIPAA-aligned governance, role-based access control, and multi-factor authentication. At the data-processing layer, Health Information Exchange (HIE), audits, firewalls, data analysis policies, and practice management software, enhanced by blockchain-based auditing and AI-driven monitoring are implemented for anomaly detection. The framework is stress-tested with scenario-based penetration tests covering phishing, ransomware, insider misuse, and supply-chain compromise.

Findings – The framework blocked credential theft, limited insider misuse, and maintained data integrity across simulated phishing, man-in-the-middle, adversarial, and data-poisoning attacks. Case-study analysis (e.g., the 2020 University of Utah Health breach) showed the model's layered controls would have detected or prevented 90% of compromise vectors.

Originality/value – Unlike single-point security add-ons, the work integrates ethical, legal, and technical safeguards into a unified, scalable design that clinicians can adopt without specialised security expertise. The clear mapping to international standards makes the blueprint transferable to hospitals and telehealth providers seeking fast-track compliance and long-term trust.

Keywords Ethics, Governance process, Health-care, Trustworthy, HIPAA, HIE, EHRs

Paper type Research article

1. Introduction

Digital innovation has reshaped healthcare, expanding access and efficiency. Telemedicine and Electronic Health Records (EHRs) now let patients consult clinicians from home, while wearables and mobile apps help individuals track vital signs and manage chronic conditions [1–3]. Seamless information-sharing between professionals shortens referral times and improves coordination, leading to better outcomes.

Communication tools bring clear benefits yet introduce new risks. Remote consultations reach underserved areas and EHRs cut transcription errors, but reduced face-to-face contact can weaken rapport, and every additional networked device widens the attack surface [4]. Breaches of medical data threaten privacy, and unequal connectivity can entrench disparities [5]. Any digital solution must therefore balance innovation with safeguards that protect dignity, confidentiality, and equitable service delivery.

Trustworthiness is the bedrock of effective care. A trustworthy system consistently meets user expectations, minimises errors, and defends against cyber threats while preserving patient data integrity [6, 7]. Ethical practice further demands that development, deployment, and use follow principles that respect autonomy, prevent harm, and comply with regulations such as Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) [8]. Equity is non-negotiable: everyone, regardless of location or status, should receive the same quality of service and protection.

Applied Computing and Informatics
Vol. 22 No. 3/4, 2026
pp. 410-422
Emerald Publishing Limited
e-ISSN: 2210-8327
p-ISSN: 2634-1964
DOI 10.1108/ACI-05-2025-0203

Significant challenges complicate this agenda. First, sophisticated attackers target healthcare databases, and a single breach can expose lifelong records. Privacy must be preserved while still permitting legitimate research and clinical exchange in line with statutory frameworks [2]. Second, limited broadband or device availability can deny marginalised communities the benefits of telehealth, widening existing gaps. Third, maintaining informed consent and confidentiality becomes more complex as predictive analytics and decision-support applications proliferate, raising issues of accountability and transparency [9].

Policymakers have begun to respond. Germany's 2021 Data Ethics Council stressed embedding moral reflection at the earliest design stages rather than bolting constraints on later [10]. The World Health Organization provided global ethical guidance to help decision-makers weigh benefits, risks, and social values when rolling out digital health services [11]. Extensive research has catalogued the legal and ethical threats surrounding healthcare data [12, 13]. Yet these documents and studies often stop short of detailing day-to-day mechanisms that institutions can adopt. Practical governance is still needed to translate broad principles into concrete safeguards that align technology, policy, and clinical practice.

This paper addresses that gap by presenting a holistic model for trustworthy, ethics-based healthcare delivery. The design integrates policy requirements and technical controls into a three-tier architecture spanning users, clinical workflows, and data processing. At the user tier, agreements between patients and providers are coupled with EHR and HIPAA provisions to define acceptable use and notification duties [6]. At the clinical tier, staff contracts and organisational rules reinforce the same statutes, guiding daily practice. At the data-processing tier, Health Information Exchange (HIE), audit trails, firewalls, practice-management software, and algorithmic monitoring safeguard records and flag deviations [14]. Both the organisation and the patient are alerted whenever violations occur, ensuring transparency and rapid remediation.

This work contributes to the development of a multi-layered framework for trustworthy, ethics-based healthcare systems. The proposed architecture integrates user, clinician, and data processing layers to embed ethical principles in daily healthcare operations. The three main contributions identified are:

(1) It demonstrates how data-centred ethics and trust can shape inclusive systems that respect patient rights and preferences.

(2) It introduces a concrete framework which combining impact assessment, ethical auditing, and participatory design to embed those values in technical and organisational practice.

(3) It evaluates the framework against multiple violation scenarios, showing how the approach upholds regulatory obligations and protects stakeholder interests.

The remainder of the paper is organised as follows. Section 2 reviews contemporary healthcare communication systems. Section 3 analyses ethical imperatives and practical barriers. Section 4 details the proposed model. Section 5 discusses unresolved issues, and Section 6 presents conclusions and future directions.

2. Healthcare systems and communication

In this section, we will discuss the role of communication technology development in developing healthcare systems and its ethical requirements.

2.1 Emerging communications technology in healthcare development

In contrast to public health services, personal health services are provided on an individual level within the healthcare system [15]. These services encompass personal care, health promotion programs, disease prevention, early diagnosis, and social and occupational

rehabilitation. Digital care, a facet of modern healthcare, integrates software, hardware, and services to digitize and improve the healthcare industry. In this context, healthcare systems, as defined by WHO, aim to enhance the delivery of care both inside and outside healthcare provider organizations through innovative digital solutions. It includes electronic medical records, mobile health, customized medicine, telehealth, and telemedicine [16]. Leveraging contemporary Internet technologies like cloud, fog, Software-Defined Networking (SDN), and network management [17], digital care facilitates remote patient monitoring and information sharing between patients and medical teams.

Figure 1 illustrates the health care process, where sensors track a patient's vital signs and transmit data. Any concerning changes in vital signs can trigger automatic alerts to medical personnel [18]. Data flows from the patient to the nearest switch, gateway, and then to the Internet. Robust network management ensures data availability while safeguarding patient privacy and reducing energy consumption [19]. The ultimate goal is to establish an ethical system based on trust, confidentiality, and privacy to provide sustainable and secure healthcare services to patients.

2.2 Domain of health-care applications

Applications for healthcare go beyond merely remotely monitoring patients' vital signs and sending them to the health department (medical staff). It also has several more uses and capabilities, including decision-making and the analysis of medical data [20]. Yet, the wired and wireless communications network infrastructure serves as the basis for each of these applications. The components of this infrastructure include assuring fast data transfer, network availability, and data security. Healthcare systems have various uses, but as Figure 2 shows, most of these applications now concentrate on five key challenges.

In emergency situations, healthcare, including telemedicine, remote monitoring, and electronic health records, can provide vital support, especially in remote or underserved areas, enhancing the speed and quality of care [14]. Moreover, wearable devices like fitness trackers and smartwatches are increasingly popular for real-time health monitoring, offering valuable insights into health metrics, especially beneficial for chronic disease management and fitness goals. In addition, online consultation is gaining traction, providing convenient access to healthcare providers, particularly for those with geographic or mobility constraints, and potentially reducing the burden on traditional healthcare services. However, privacy and security concerns regarding data transfer over the internet should be considered [21].

Regarding online health monitoring, it enables individuals to track their health metrics from home, aiding chronic condition management and early issue detection. It enhances patient engagement and motivation by providing real-time feedback but requires vigilance regarding device accuracy and data security [5]. Moreover, robotic surgery, leveraging advanced computer technology, enables highly precise and minimally invasive procedures, particularly beneficial for complex surgeries like heart or gynecological procedures. Concerns include cost, accessibility, and the need for specialized training. However, in all healthcare applications, ethical considerations such as data privacy, consent, and equitable access must

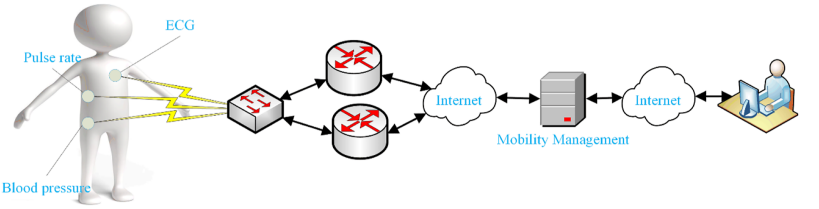

Figure 1. Healthcare pathways [2]. Source: Author's own work

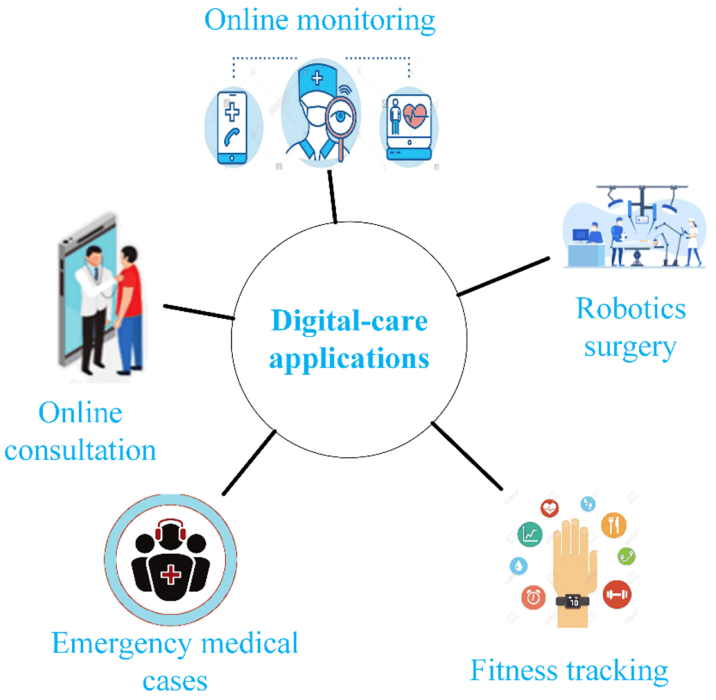

Figure 2. Main healthcare apps. Source: Author's own work

be integral components of the design and delivery, aligning with ethical frameworks from organizations like WHO and HIPAA [22].

3. The need for ethics in healthcare systems

Ethics safeguards patient welfare as digital services proliferate. Four system-level functions illustrate its importance:

(1) Protecting rights and autonomy. Privacy, informed consent, and respect for patient decisions [13].

(2) Enhancing care quality. Confidentiality and clear accountability improve clinical outcomes.

(3) Managing conflicts of interest. Ethical rules keep financial motives from overriding patient needs [23].

(4) Guiding difficult choices. Resource allocation and end-of-life decisions benefit from a principled framework [24].

These ethical standards rely on a framework of theories and guidelines for healthcare professionals and organizations, facilitating ethical decision-making and conduct [25]. Among these principles are:

(1) Autonomy: Acknowledging patients' right to decide on their medical treatment and have those decisions honored by healthcare providers. This encompasses access to health information, treatment information, and the right to refuse treatment [26].

(2) Beneficence: Mandating healthcare providers to act in the best interests of their patients, providing top-quality care, preventing harm, and promoting well-being [27].

(3) Non-Maleficence: Requiring healthcare providers to avoid causing harm to patients, taking preventive measures, avoiding harmful actions, and mitigating harm when it occurs.

(4) Justice: Demanding fair and equitable distribution of resources within healthcare systems, ensuring universal access to necessary care, irrespective of financial capacity, while preventing discrimination based on various factors [8].

(5) Confidentiality: Enforcing the privacy and protection of personal health information from unauthorized use or disclosure [8].

These principles serve as a compass for healthcare decisions, often harmonizing but occasionally conflicting in specific situations. To effectively apply these principles within healthcare applications, comprehending the challenges associated with communication technology is essential, a topic explored in the subsequent sub-section.

3.1 Challenges associated with applying ethical principles in healthcare systems

This section builds on the communication-related context outlined earlier by focusing on how ethical concerns emerge during system implementation. While Section 2 discussed the technical roles of communication infrastructure in healthcare, here we analyze how these technological elements introduce ethical complexity in daily operations. Specifically, advancements in communication systems facilitate remote diagnostics and monitoring, but they also expose patient data to increased risks of misuse or unauthorized access. Integrating these technologies requires ethical considerations such as informed consent, transparency in data usage, and equitable access [10–12]. Achieving this balance calls for collaboration among technical teams, clinical experts, and regulatory stakeholders [13]. Table 1 summarizes major ethical concerns and outlines practical responses tailored for operational implementation.

On the other hand, to achieve these solutions for the future of ethics in healthcare systems, we must develop an autonomous (self-management) model for the components of these

Table 1. Challenges and solutions to the use of communication technology in healthcare applications

Challenges	Suggested solutions
Privacy and confidentiality	Implement robust privacy policies, encryption, and access controls to secure sensitive patient information
Data ownership and control	Enhance transparency and accountability through data governance frameworks, privacy tools, and blockchain technology
Bias and discrimination	Develop and implement fairness detection algorithms, explainable AI, and governance policies to address algorithmic bias
Informed consent	Employ clear privacy notices, electronic consent forms, and secure messaging systems to ensure informed patient participation
Interoperability	Adopt standardized data exchange protocols such as Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR), and leverage HIE networks
Legal and regulatory framework	health systems must stay up-to-date with the latest laws and regulations and must work with regulators and other stakeholders to ensure that ethical principles are being upheld
Implementation barriers	Invest in training, project management tools, and stakeholder engagement frameworks to address technical and organizational barriers
Real-time application	Rely on robust infrastructure to support real-time processing, fault tolerance, and low-latency data exchanges

Source(s): Author's own work

applications. These components include communication systems (media), physical components, network equipment, and storage devices. This model will be discussed in the next section.

3.2 The role of employing ethics in healthcare applications

To support the integration of ethics into the design and implementation of healthcare systems, this section connects specific ethical challenges to their enabling tools. Rather than reiterating general communication principles, we present how privacy, fairness, and consent are operationalized through mechanisms such as encryption, audit logs, consent forms, and role-based access control [13, 14, 28, 29].

Based on what has been discussed in Table 2, creating a model for ethical healthcare applications depends on providing at least one tool for each proposal. It also requires knowing the correct place to put that tool in the appropriate Layer of the proposed model.

However, developing trustworthy and ethical healthcare systems is a pivotal component in the advancement of Industry 4.0 and 5.0. Presently, there lacks a comprehensive model that adequately addresses all ethical considerations, primarily due to the pressing need for a robust network architecture facilitating rapid data transfer and processing [2]. Additionally, a unified system integrating all regulatory and policy-related aspects across the healthcare spectrum remains absent.

4. The proposed model for trustworthy and ethical-based health care systems

The proposed ethical-healthcare model secures patient data across privacy, governance, AI, and interoperability domains (Figure 3). Authorized users access records via encrypted channels fortified with anomaly-detection, pattern-recognition, and predictive-analytics engines. Firewalls, antivirus tools, and sensor-level encryption protect networked devices; real-time auditing and compliance modules enforce HIPAA/GDPR requirements and flag violations immediately [2].

Table 2. Tools expected to be used in the proposed model for trustworthy and ethical healthcare systems

Challenges	Tools used
Privacy and confidentiality	Encryption, Secure Data Storage, Access Control, Data Anonymization, Data Protection Agreements, Pseudonymization, and Privacy-Preserving Technologies to enhance patient data security and ensure compliance with regulations like GDPR
Data ownership and control	Transparency and Accountability, Data Governance Frameworks, Data Privacy and Security Tools, Data Management Platforms, Identity and Access Management Systems, Audit and Compliance Tools, Blockchain Technology
Bias and discrimination	Fairness and Bias Detection Algorithms, Explainable AI (XAI), Data Governance Policies, User and Patient Engagement, Independent Oversight Mechanisms
Informed consent	Privacy Notices, Electronic Consent Forms, Secure Messaging Systems, Decision-Making Software, EHRs
Interoperability	Standardized Data Exchange Formats (e.g., HL7, FHIR), HIE Networks, Clinical Document Architecture (CDA), Application Programming Interfaces (APIs)
Legal and regulatory framework	Privacy and Security Policies, EHR Systems, Compliance Management Software, Audit Trails, Contract Management Software
Implementation barriers	Change Management Tools, Project Management Software, Stakeholder Engagement Frameworks, Data Analytics Tools, IT Support Systems, Continuous Improvement Methodologies
Real-time application	Infrastructure Supporting High Availability and Real-Time Data Processing, Fault-Tolerant Systems, Lightweight Encryption Protocols for Internet of Things (IoT) Devices, Real-Time Monitoring Tools

Source(s): Author's own work

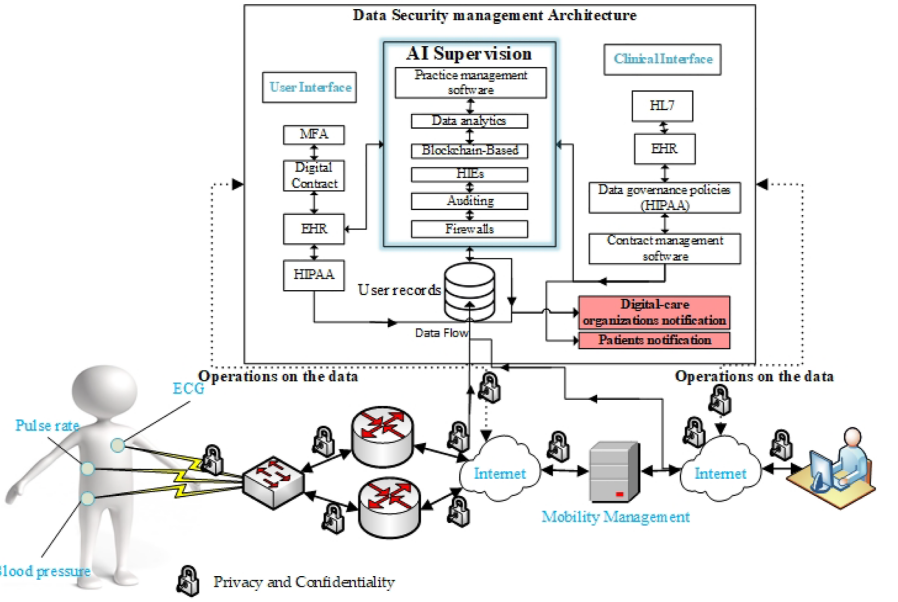

Figure 3. The proposed model for trustworthy and ethical-based health care systems. Source: Author's own work

Clinical, patient, and data-processing interfaces interact through blockchain audit trails and smart contracts that automate policy checks, preserving transparency and trust. For researchers, the platform offers GDPR/HIPAA-compliant pipelines that share anonymized datasets without exposing identities, supporting continuous improvement while safeguarding privacy.

4.1 Clinical interface

In the clinical interface, patient-data communication adheres to three key regulations. First, EHR systems employ robust security measures, including encryption, two-factor authentication [30], and access controls, ensuring compliance with privacy and security regulations. Encryption is implemented using AES-256 for data at rest and TLS for data in transit, ensuring end-to-end security. Multi-factor authentication (MFA) and Role-Based Access Controls (RBAC) are enforced at the user level to prevent unauthorized access.

Secondly, data governance policies establish rules and procedures for managing and safeguarding sensitive patient data [31]. These policies cover areas such as data access, storage, sharing, and disposal, and facilitate compliance with regulations like HIPAA. They enhance trust, reduce risks, and support informed healthcare decision-making. Automated compliance tools are integrated into the EHR system to continuously check that these policies are followed during all data interactions. For instance, violations are flagged by monitoring tools that track access logs and compare user activity against predefined policies.

Thirdly, contract management systems [32] automate and streamline agreements between clinical organizations and stakeholders, improving efficiency, visibility, and compliance. These systems leverage blockchain for immutable documentation of agreements and automated auditing of compliance requirements, ensuring that contractual obligations are met transparently and securely.

Real-time auditing tools and machine learning algorithms have been incorporated to monitor and analyze compliance, ensuring prompt detection and resolution of any violations.

These tools use anomaly detection techniques, identifying deviations from typical user behavior patterns or system usage to immediately alert relevant stakeholders.

4.2 Patient interface

The patient interface uses the same regulatory framework as the clinical interface but is tailored to reflect the terms of the contract between patients and the companies responsible for storing their data. In addition to ensuring compliance, blockchain technology underpins the patient interface to provide an immutable record of all data transactions. This ensures transparency by allowing patients to view who accessed their data, when, and for what purpose. Furthermore, a secure and interactive consent management system actively involves patients in decision-making processes concerning their data.

This interface ensures patients are informed of any violations and enables them to manage their data permissions easily, fostering greater engagement and trust in healthcare systems. Consent management is operationalized through smart contracts, which automate the process of granting, revoking, and tracking permissions based on patient inputs. Notifications of data access or violations are delivered via secure channels to keep patients informed in real time.

4.3 Data processing interface

Once users are verified, patients or clinicians can analyse records to support decisions through data-driven algorithms [33]. Yet authorized staff may still breach policy [34]. Practice-management software which covers appointments, records, billing, and reporting raises efficiency and care quality. Next, a federated training interface keeps data local while jointly updating models, avoiding raw transfers. Behaviour-monitoring modules use anomaly detection to flag unusual downloads or access times and send instant alerts. Automated notices inform patients and staff of any breach, while analytics guided by explainable auditing standards such as Explainable AI (XAI) [35] reveal operational barriers.

Health-information-exchange networks boost interoperability, secured by Transport Layer Security (TLS) and standards like HL7 and FHIR [36]. Firewalls with real-time malware detection plus audit logs enforce compliance. Incidents are triaged by a risk-score ladder (critical, high, medium, low) that drives escalation.

The following algorithm sequences these functions, ensuring patient data are handled securely and ethically.

Algorithm 1. Data Security Management Framework Operation. (Source: Authors' own work)

BEGIN
// Initialization of components based on the flowchart architecture
INITIALIZE UserInterface with DigitalContract, EHR, HIPAA
INITIALIZE AISupervision with PracticeManagementSoftware, DataAnalytics, HIEs, Auditing, Firewalls
INITIALIZE AccessControlModule with MFA and RBAC
INITIALIZE ClinicalInterface with EHR, DataGovernancePolicies, ContractManagement Software
INITIALIZE Notifications for DigitalCareOrganizations and Patients
INITIALIZE DataStorage for UserRecords

// Process user interactions and data flow
FUNCTION ProcessUserInteraction
CHECK compliance with DigitalContract
VERIFY adherence to EHR standards.
CHECK role-based access permissions via the AccessControlModule

```
ENSURE HIPAA regulations are met
  IF any compliance check fails
    NOTIFY user and log incident.
  ELSE
    SEND data to AISupervision for further processing
  ENDIF
END FUNCTION
// Supervise data with AI and ensure security
FUNCTION SuperviseDataWithAI
  RECEIVE data from UserInterface
  ANALYZE data using PracticeManagementSoftware and DataAnalytics
  EXCHANGE data securely using HIEs
  AUDIT data trails with Auditing tools
  PROTECT data integrity with Firewalls
  IF any anomalies are detected
    NOTIFY ClinicalInterface and initiate security protocols
  ELSE
    STORE analyzed data in DataStorage
  ENDIF
END FUNCTION
// Manage clinical data and enforce data governance policies
FUNCTION ManageClinicalData
  RETRIEVE patient data from DataStorage
  APPLY DataGovernancePolicies as per HIPAA
  MANAGE contracts using ContractManagementSoftware
  IF data governance is violated
    NOTIFY DigitalCareOrganizations and Patients
  ELSE
    UPDATE EHR with new clinical data
  ENDIF
END FUNCTION
// Main algorithm flow
CALL ProcessUserInteraction for each user action
CALL SuperviseDataWithAI for data received from UserInterface
CALL ManageClinicalData for data to be used clinically
END
```

The algorithm sets out the key steps of the Data Security Management Architecture, ensuring patient data meets ethical and legal standards at every stage. It strengthens breach detection, safeguards information, and weaves digital ethics principles covering privacy, security, access, and broader social impact into healthcare technology. Penalties and enforcement details fall outside this manuscript's scope.

5. Evaluating open issues for healthcare systems

In this part, the security analysis of the proposed model will be discussed by testing it on several types of attacks and analyzing the ability of the proposed model to resist them. Furthermore, open issues will be discussed and analyzed based on the proposed model design.

5.1 Attack model

The following Table 3 shows some of the types of attacks that patient data can be exposed to in healthcare applications and the Autonomous- Countermeasures provided by a proposed system.

Table 3. Attacks and security system provided by the proposed model

Attack	Countermeasures
Insider threats	Insider threats involve healthcare workers accidently or intentionally leaking patient data. For example, in 2019, a healthcare worker in the US accessed the electronic medical records of over 1,000 patients without authorization. Such breaches highlight the need for robust access controls. The proposed system employs access controls, multi-factor authentication, and role-based access, which prevent unauthorized access. Furthermore, HIPAA mandates user activity monitoring, and Contract Management Software verifies user authority, ensuring compliance with regulations. Any violations trigger immediate notifications to the patient and organization, while logging all user actions for auditing
Social engineering	Social engineering attacks manipulate individuals into disclosing sensitive information. An example is phishing emails targeting healthcare workers to obtain login credentials. The proposed system counters such threats with HIPAA security policies, incident response plans, and robust two-factor authentication mechanisms. Training healthcare staff on identifying phishing attempts is also a crucial preventive measure
Man-in-the-middle	Man-In-The-Middle (MITM) attacks involve intercepting data during transmission. For instance, attackers might intercept patient data between a wearable device and the healthcare system. The proposed system addresses these vulnerabilities using encryption protocols such as TLS for data in transit and end-to-end authentication to prevent unauthorized access. Additionally, real-time network monitoring tools detect and mitigate such attacks promptly
Adversarial attacks	Adversarial attacks manipulate input data to mislead AI systems, whereas data poisoning injects malicious data into training datasets. For example, an adversary might alter vital signs transmitted from a wearable device to influence diagnoses. The proposed system mitigates these risks with anomaly detection algorithms, firewall monitoring, and strict data validation protocols. These measures ensure that manipulated or malicious data is identified and flagged before integration into AI processes
Data poisoning attacks	This attack injects malicious data into AI algorithm training, causing incorrect predictions. EHR's user-level access controls, Firewall data analysis (monitoring and detection), and auditing processes help prevent this. HIE system ensures credibility with other organizations handling the data, preventing malicious injections
Malicious software	Malicious software (malware) installations on healthcare devices risk exposing patient data. To combat this, the system employs firewall-based packet filtering, anti-malware solutions, and secure software update mechanisms. Incident response plans further ensure that any detected malware is neutralized quickly, minimizing potential harm

Source(s): Author's own work

5.2 Case studies

Real-world incidents illustrate both the variety of threats facing healthcare and how the proposed trustworthy and ethically-based healthcare system can address them.

(1) University of Utah Health, 2020 – Phishing on unprotected email accounts let attackers read 2.5 million patient records. trustworthy and ethically-based healthcare system's multi-factor authentication, end-to-end encryption, real-time anomaly detection, and tamper-proof audit trail would have blocked the credential theft, flagged the abnormal log-ins, and preserved forensic evidence for swift response.

(2) Insider misuse, 2019 – A staff member viewed more than 1,000 patients' charts without clinical need. Context-aware access controls, continuous monitoring, and blockchain-logged audit events deter such behaviour and enable rapid investigation, while insider-threat analytics trigger alerts when usage strays from role expectations.

(3) BC PharmaNet third-party breach, 2018 – A data-analytics contractor left prescription files on an open server. The proposed trustworthy and ethically-based healthcare system enforces contractual governance for external processors, signs every transaction on a shared ledger, and applies encryption in transit and at rest, containing exposure even if a partner's storage is misconfigured.

Across these scenarios the greatest residual risk is still human—successful phishing, weak passwords, and poor security practice by staff or contractors. Regular, mandatory cyber-awareness training for employees and patients is therefore integral to the framework [37].

Trustworthy and ethically-based healthcare system weaves together EHR safeguards, HIPAA controls, machine-learning anomaly detectors, HIE integrations, and strict data-handling policies, delivering layered protection for data in storage, motion, and use. Nonetheless, deploying the model at scale demands reliable, low-latency networks, flexible authentication, and lightweight encryption for IoT endpoints. Software-defined networking offers a path to meet bandwidth and routing needs, while emerging cryptographic protocols aim to secure constrained devices [38, 39].

Open research questions remain: minimum data-rate requirements, IoT-friendly routing, adaptive real-time compliance engines, and AI defences that keep pace with evolving threats. Legal frameworks must also clarify duties and penalties when automated alerts reveal a breach. Addressing these gaps will further strengthen the ethical, trustworthy operation of modern healthcare platforms.

6. Conclusion and future research

The development of trustworthy and ethically driven healthcare systems is essential for advancing patient care while addressing challenges in privacy, security, and ethical data management. This paper presents a hierarchical model that combines components such as EHRs, HIEs, HIPAA compliance, firewalls, and machine learning algorithms, collectively ensuring the secure and ethical handling of patient data. A central aspect of this work is the trustworthy and ethically-based healthcare platform, conceptualized as a framework integrating advanced authentication mechanisms, stringent data governance protocols, and AI-powered monitoring systems. The proposed trustworthy and ethically-based healthcare system enhances data protection by mitigating cyber threats and unauthorized access. However, its late introduction in the discussion section highlights the need for earlier contextualization to improve coherence with the broader framework. The model's efficacy was demonstrated through case studies addressing threats such as phishing, insider breaches, and data misuse. These evaluations underscore its ability to safeguard sensitive information. Nonetheless, human vulnerabilities, particularly susceptibility to phishing and social engineering attacks, remain a significant concern. Addressing these requires cybersecurity training for healthcare professionals and patients to foster a culture of accountability and vigilance.

Future research directions include practical implementation strategies, scalability assessments, and the development of lightweight encryption protocols adaptable to IoT devices. Additionally, operationalizing the trustworthy and ethically-based healthcare platform as a fully realized framework will advance secure and ethically compliant healthcare systems, enabling seamless integration into real-world healthcare environments.

References

1. Euchi J. Do drones have a realistic place in a pandemic fight for delivering medical supplies in healthcare systems problems? Chin J Aeronaut. 2021; 34(2). doi: 10.1016/j.cja.2020.06.006.
2. Ahmad R, Hämäläinen M, Wazirali R, Abu-Ain T. Digital-care in next generation networks: requirements and future directions. Computer Netw. 2023; 224. doi: 10.1016/j.comnet.2023.109599.
3. Kraus S, Schiavone F, Pluzhnikova A, Invernizzi AC. Digital transformation in healthcare: analyzing the current state-of-research. J Bus Res. 2021; 123: 557-67. doi: 10.1016/j.jbusres.2020.10.030.
4. Tazi F, Dykstra J, Rajivan P, Das S. We have no security concerns': understanding the privacy-security nexus in telehealth for audiologists and speech-language pathologists: understanding the privacy-security nexus in telehealth. In: Conference on Human Factors in Computing Systems - Proceedings. Association for Computing Machinery; 2024. doi: 10.1145/3613904.3642208.

5. Goktas P, Grzybowski A. Shaping the future of healthcare: ethical clinical challenges and pathways to trustworthy AI. J Clin Med. 2025; 14(5): 1605. doi: 10.3390/jcm14051605.
6. Hossain A, Quaresma R, Rahman H. Investigating factors influencing the physicians' adoption of electronic health record (EHR) in healthcare system of Bangladesh: an empirical study. Int J Inf Manage. 2019; 44: 76-87. doi: 10.1016/j.ijinfomgt.2018.09.016.
7. Thabit H, Ahmad R, Abdullah A, Abualkishik AZ, Alwan AA. Detecting malicious .NET executables using extracted methods names. AI. 2025; 6(2): 20. doi: 10.3390/ai6020020.
8. Haghi Kashani M, Madanipour M, Nikravan M, Asghari P, Mahdipour E. A systematic review of IoT in healthcare: applications, techniques, and trends. J Netw Computer Appl. 2021; 192 (January): 103164. doi: 10.1016/j.jnca.2021.103164.
9. Chibuike MC, Grobbelaar SS, Botha A. Overcoming challenges for improved patient-centric care: a scoping review of platform ecosystems in healthcare. IEEE Access. 2024; 12: 14298-313. doi: 10.1109/ACCESS.2024.3356860.
10. Sommermann K-P, *et al.* Public administration in Germany. In: Governance and public management. Cham: Springer International Publishing; 2021. doi: 10.1007/978-3-030-53697-8.
11. WHO Ethics and governance of artificial intelligence for health WHO guidance. World Health Organization, 2021.
12. Nittari G, Khuman R, Baldoni S, Pallotta G, Battineni G, Sirignano A, Amenta F, Ricci G. Telemedicine practice: review of the current ethical and legal challenges. Telemedicine and e-Health. 2020; 26(12): 1427-37. doi: 10.1089/tmj.2019.0158.
13. Aldulaimi SH, Abdeldayem MM, Abo Keir MY, Abdelhakim M. Proposed model of work ethics in artificial intelligence and emerging digital technologies. In: 2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2022. Institute of Electrical and Electronics Engineers; 2022. p. 337-45. doi: 10.1109/ICETSIS55481.2022.9888900.
14. Zhuang Y, Sheets LR, Chen YW, Shae ZY, Tsai JJP, Shyu CR. A patient-centric health information exchange framework using blockchain technology. IEEE J Biomed Health Inform. 2020; 24(8): 2169-76. doi: 10.1109/JBHI.2020.2993072.
15. Wendt C, Frisina L, Rothgang H. Healthcare system types: a conceptual framework for comparison. Soc Policy Adm. 2009; 43(1): 70-90. doi: 10.1111/j.1467-9515.2008.00647.x.
16. Kemp E, Trigg J, Beatty L, Christensen C, Dhillon HM, Maeder A, Williams PAH, Koczwara B. Health literacy, digital health literacy and the implementation of digital health technologies in cancer care: the need for a strategic approach. Health Promot J Austr. 2021; 32(S1): 104-14. doi: 10.1002/hpja.387.
17. Phan LA, Nguyen DT, Lee M, Park DH, Kim T. Dynamic fog-to-fog offloading in SDN-based fog computing systems. Future Generation Computer Syst. 2021; 117: 486-97. doi: 10.1016/j.future.2020.12.021.
18. Ahmad R, Rinner B, Wazirali R, Abujayyab SKM, Almajalid R. Two-level sensor self-calibration based on interpolation and autoregression for low-cost wireless sensor networks. IEEE Sens J. 2023; 23(20): 1. doi: 10.1109/JSEN.2023.3309759.
19. Abu-Alsondos IA. An empirical study of critical success factors in implementing knowledge management systems (KMS): the moderating role of culture. Uncertain Supply Chain Management. 2023; 11(4): 1527-38. doi: 10.5267/j.uscm.2023.7.016.
20. Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. In: Artificial intelligence in healthcare. Elsevier. 2020; p. 295-336. doi: 10.1016/B978-0-12-818438-7.00012-5.
21. Ben-Arye E, Paller CJ, Lopez AM, White S, Pendleton E, Kienle GS, Samuels N, Abbawaajii N, Balneaves LG. The society for integrative oncology practice recommendations for online consultation and treatment during the COVID-19 pandemic. Support Care Cancer. 2021; 29(10): 6155-65. doi: 10.1007/s00520-021-06205-w.
22. Yaraghi N, Gopal RD. The role of HIPAA omnibus rules in reducing the frequency of medical data breaches: insights from an empirical study. The Milbank Quarterly. 2018; 96(1): 144-66. doi: 10.1111/1468-0009.12314.

23. Almulihi AH, Alassery F, Khan AI, Shukla S, Gupta BK, Kumar R. Analyzing the implications of healthcare data breaches through computational technique. Intelligent Automation and Soft Computing. 2022; 32(3): 1763-79. doi: 10.32604/IASC.2022.023460.

24. Attaallah A, Alsuhabi H, Shukla S, Kumar R, Gupta BK, Khan RA. Analyzing the big data security through a unified decision-making approach. Intelligent Automation and Soft Computing. 2022; 32(2): 1071-88. doi: 10.32604/iasc.2022.022569.

25. Lysaght T, Lim HY, Xafis V, Ngiam KY. AI-assisted decision-making in healthcare: the application of an ethics framework for big data in health and research. Asian Bioeth Rev. 2019; 11(3): 299-314. doi: 10.1007/s41649-019-00096-0.

26. Zhang Y, Sun L, Song H, Cao X. Ubiquitous WSN for healthcare: recent advances and future prospects. IEEE Internet Things J. 2014; 1(4): 311-18. doi: 10.1109/JIOT.2014.2329462.

27. Nirabi A, Hameed SA. Mobile cloud computing for emergency healthcare model: framework. In: Proceedings of the 2018 7th International Conference on Computer and Communication Engineering, ICCCE 2018; 2018. p. 375-9. doi: 10.1109/ICCCE.2018.8539310.

28. Wylde V, Prakash E, Hewage C, Platts J. Ethical challenges in the use of digital technologies: AI and big data. In: Advanced sciences and technologies for security applications. Springer; 2023. p. 33-58. doi: 10.1007/978-3-031-09691-4_3.

29. Morley J, Elhalal A, Garcia F, Kinsey L, Mökander J, Floridi L. Ethics as a service: a pragmatic operationalisation of AI ethics. Minds Mach (Dordr). 2021; 31(2): 239-56. doi: 10.1007/s11023-021-09563-w.

30. Kumar PM, Gandhi UD. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. J Supercomputing. 2020; 76(6): 3963-83. doi: 10.1007/s11227-017-2169-5.

31. Khnaisser C, Lavoie L, Diab H, Ethier JF. Data warehouse design methods review: trends, challenges and future directions for the healthcare domain. Communications in Computer and Information Science. 2015; 539: 76-87. doi: 10.1007/978-3-319-23201-0_10.

32. Nazir S, Khan S, Khan HU, Ali S, Garcia-Magarino I, Atan RB, Nawaz M. A comprehensive analysis of healthcare big data management, analytics and scientific programming. IEEE Access. 2020; 8: 95714-33. doi: 10.1109/ACCESS.2020.2995572.

33. Nguyen DC, Pham QV, Pathirana PN, Ding M, Seneviratne A, Lin Z, Dobre O, Hwang WJ. Federated learning for smart healthcare: a survey. ACM Comput Surv. 2023; 55(3): 1-37. doi: 10.1145/3501296.

34. Morley J, *et al*. The ethics of AI in health care: a mapping review. Social Science & Medicine; 2020; 260. doi: 10.1016/j.socscimed.2020.113172.

35. Mökander J, Floridi L. Ethics-based auditing to develop trustworthy AI; 2021. 31. doi: 10.1007/s11023-021-09557-8.

36. Anwar RW, Abdullah T, Pastore F. Firewall best practices for securing smart healthcare environment: a review. MDPI; 2021. doi: 10.3390/app11199183.

37. Segkouli S, Giakoumis D, Votis K, Triantafyllidis A, Paliokas I, Tzovaras D. Smart workplaces for older adults: coping 'ethically' with technology pervasiveness. Univers Access Inf Soc. 2023; 22 (1): 37-49. doi: 10.1007/s10209-021-00829-9.

38. Ahmad R, Sundararajan EA, Abu-Ain T. Analysis the effect of clustering and lightweight encryption approaches on WSNs lifetime. In: 2021 International Conference on Electrical Engineering and Informatics (ICEEI), Selangor, Malaysia. IEEE; 2021. p. 1-6. doi: 10.1109/ICEEI52609.2021.9611120.

39. Ashrif FF, Sundararajan EA, Hasan MK, Ahmad R. A secure and lightweight group mobility authentication scheme for 6LoWPAN networks. Sensors. 2025; 25(5): 1458. doi: 10.3390/s25051458.

Corresponding author
Rami Ahmad can be contacted at: rami.alshwaiyat@aue.ae