Cureus
Part of SPRINGER NATURE

Open Access Review Article

Digital Health Policy and Cybersecurity Regulations Regarding Artificial Intelligence (AI) Implementation in Healthcare

Review began 01/17/2025
Review ended 02/11/2025
Published 03/16/2025

DOI: 10.7759/cureus.80676

Abdullah Virk [1], Safanah Alasmari [2], Deepkumar Patel [3], Karen Allison [1]

1. Department of Ophthalmology, Flaum Eye Institute, University of Rochester, Rochester, USA 2. School of Health Sciences and Practice, New York Medical College, New York, USA 3. Department of Public Health, School of Health Science and Practice, New York Medical College, Valhalla, USA

Corresponding author: Deepkumar Patel, deepkumarptl@gmail.com

Abstract

The landscape of healthcare is rapidly changing with the increasing usage of machine and deep learning artificial intelligence and digital tools to assist in various sectors. This study aims to analyze the feasibility of the implementation of artificial intelligence (AI) models into healthcare systems. This review included English-language publications from databases such as SCOPUS, PubMed, and Google Scholar between 2000 and 2024. AI integration in healthcare systems will assist in large-scale dataset analysis, access to healthcare information, surgery data and simulation, and clinical decision-making in addition to many other healthcare services. However, with the reliance on AI, issues regarding medical liability, cybersecurity, and health disparities can form. This necessitates updates and transparency on health policy, AI training, and cybersecurity measures. To support the implementation of AI in healthcare, transparency regarding AI algorithm training and analytical approaches is key to allowing physicians to trust and make informed decisions about the applicability of AI results. Transparency will also allow healthcare systems to adapt appropriately, provide AI services, and create viable security measures. Furthermore, the increased diversity of data used in AI algorithm training will allow for greater generalizability of AI solutions in patient care. With the growth of AI usage and interaction with patient data, security measures and safeguards, such as system monitoring and cybersecurity training, should take precedence. Stricter digital policy and data protection guidelines will add additional layers of security for patient data. This collaboration will further bolster security measures amongst different regions and healthcare systems in addition to providing more means to innovative care. With the growing digitization of healthcare, advancing cybersecurity will allow effective and safe implementation of AI and other digital systems into healthcare and can improve the safety of patients and their personal health information.

Categories: Public Health, Healthcare Technology, Health Policy
Keywords: ai and digital systems, ai governance, cybersecurity and healthcare, digital healthcare systems, healthcare disparities and digital health records, patient data security, racial and ethnicity bias. discrimination

Introduction And Background

The rapid advancement in the healthcare industry has been a catalyst for increased usage of many new forms of technologies in the field. Artificial intelligence (AI) is becoming more widely used in patient care through robotic surgeries, predictive models for diagnoses, and personalized treatment plans. In addition to the usage of digital tools in patient care, advanced devices and artificial intelligence have been used in many other sectors, such as research analysis, logistics, and data collection [1]. This increase in digitalization and usage of new technologies and devices in healthcare can pave the way for new cybersecurity threats. Especially with AI having access to large amounts of private health information, it could become a target for numerous cyberattacks, potentially jeopardizing patient safety. [1,2]. Therefore, it is critical to understand the implications of AI in order to properly implement it in a way that can avoid unnecessary cybersecurity risks while maximizing the productivity of the workforce and the benefits to the patients.

Review

This review of literature included a comprehensive search of English-language publications from peer-reviewed journals in databases such as SCOPUS, PubMed, and Google Scholar between the years 2000 to 2024. Keywords used for the article search included artificial intelligence, healthcare, cybersecurity, liability, disparities, digital health policies, and ethics. Additional sources were also identified through the reference sections of the searched articles. Policy and news information was collected through government sites and reliable news organizations to discuss recent events and legislation.

AI integration in healthcare

Artificial intelligence is used in various sectors of healthcare including medical research, disease diagnosis, health monitoring, and patient care. One of the most widely used applications of AI is diagnostic analysis for screenings in which it can help physicians analyze tests such as MRIs, X-rays, and CT scans in order to provide faster and more accurate diagnoses [1]. Machine learning, where the AI model can learn and improve from the data available, and deep learning, where AI can learn and continuously improve by itself through artificial neural networks, is used in many diagnostic settings to extract findings and abnormalities. AI algorithms designed for specific medical fields analyze large datasets to find patterns, abnormalities, and the eventual diagnosis [4,5]. In ophthalmology, deep learning has become a vital factor in analyzing ocular conditions such as diabetic retinopathy through large datasets and fundus photos [5]. In mammography, AI support helped radiologists improve their detection performance with increased sensitivity and specificity for cancer screening [6]. Other diagnostic uses of AI include predicting prognosis and therapeutic response based on histological findings in pathology, and improving clinical workflow. Companies are involved in the development of AI tools such as such as HALO™ (Indica Labs, New Mexico), Oncotopix® (Visiopharm, Denmark), and DeepLens (Amazon Web Services, USA) to detect and diagnose cancers, with many other initiatives being led throughout the various fields of medicine [7].

AI-driven robotics are also significant for surgical operations since these devices provide greater accuracy and faster recovery times. Robotic-assisted surgeries have made valuable contributions to many fields of medicine. In knee arthroplasty, robotic-assisted surgery had lower revision rates, lower systemic complications, lower opiate use for postoperative pain, and decreased occurrences of manipulation under anesthesia, which is a procedure to help regain motion if the knee replacement is stiff [8,9]. AI-powered robotic-assisted surgery is emerging as a significant advancement in medicine. With the extensive amount of global regulatory policies concerning data security and patient privacy, it is paramount to evaluate the applicability of all the regulations in assessing procedures such as cardiac surgery. An example is heart bypass operations performed with the Da Vinci robot, which allows for minimally invasive procedures with fewer complications [10]. Another usage of AI in medical care is through AI-powered chatbots such as Woebot or ChatPal, which allow instant access to medical information through natural language processing (NLP) [11,12]. This allows patients and clinicians to obtain quick access to medical information and recommendations, which can help reduce the workload for many physicians [1].

Artificial intelligence usage has also been implemented in patient monitoring as well with artificial information of things (AIoT) medical devices such as wearable health sensors. AI algorithms can constantly analyze vitals and compare with large amounts of health metric data to possibly predict future problems or signs of decline [5,13]. Machine learning techniques enable AI algorithms to also adapt to human behaviors in order to identify any abnormalities and provide more personalized monitoring.

Furthermore, AI use in medical research comes with many benefits. AI can analyze large data sets without using as much time and resources as manual analysis would usually take. AI can also identify certain patterns that would have gone unnoticed in addition to forming predictions and analyzing clinical relationships [1,14]. These predictive models can have large impacts on society, such as through disease spread models and contact tracing those who have been in exposed areas to inform people to quarantine, as seen in the COVID-19 pandemic [15]. Additionally, AI use has led to many advancements in genomics and drug discovery through large-scale predictive models and data analysis [1,14]. AI usage will continue to grow with the growing interest in analyzing large-scale data sets to acquire a deeper understanding of population health or certain questions that would require lengthy analysis.

Artificial intelligence models have also been shown to assist with cybersecurity by detecting phishing attacks [16]. With a majority of medical-based emails being automatically generated communication from the hospital or labs to confirm appointments or communicate results, increased amounts of cybercriminals are trying to replicate this form of communication in order to gain access to personal information. By understanding and detecting the patterns in phishing attacks or malware-infected emails, AI can collect data to find trends in phishing data and emails. From there, any future emails that have a similar pattern are classified and automatically filtered to spam to protect the individual and company data. Moreover, AI is able to proactively help with real-time monitoring of security risks and managing assets by determining vulnerabilities in the system and finding patterns or anomalies that indicate a security risk [17]. Antivirus or antimalware applications that are powered by AI software are also used in many industries to detect thousands of files to find malware. With regards to data protection, AI can monitor data movement and user activity to determine potential threats, violations of patient privacy and Health Insurance Portability and Accountability Act (HIPAA), and leaks based on intelligence data. Additionally, AI systems can quickly mitigate the spread of a virus or threat by isolating devices, which is especially useful in clinical sectors with large amounts of private health information. Further improvements can be recommended from security reports generated by AI algorithms, which will assist in any updates to security systems and protocols [17].

Digital health policies analysis

Cybersecurity regulations and health policies are crucial in providing a framework for the integration of AI and healthcare. Digital health policies are rules and regulations that address various technological integrations among healthcare which include telemedicine, health devices, and AI. For example, in the United States, HIPAA provided a revolutionary framework for protecting patient data and confidentiality but was passed before the widespread adoption of AI in healthcare [18]. While HIPAA focuses on individual identifiers, it may not adequately address issues pertaining to AI, such as the threat of re-identification of already anonymized data. This is only worsened when the data is handled by private entities due to poorer protection of privacy, risking the nature of patient confidentiality if data can be re-identified [19]. Still, these policies can be critical building blocks in the regulation of the increasingly AI-reliant healthcare system. Similar to HIPAA, the European Union General Data Protection Regulation (GDPR) also focuses on data protection and privacy but regulates AI partially by protecting individuals from solely automated decision-making and processing of health data unless consent was obtained [20]. However, regulatory bodies like the EU are proposing policies such as the AI Act that complement existing health policies in addition to building an advanced legal framework for the development and application of AI products [20]. By using existing policies as a framework, countries and institutions can create new revisions or policies that apply to the modern landscape of healthcare. Due to the rapid digitalization of various industries, there are different digital health policies around the world, each with varying strengths and limitations (Table *1*) [21-26].

Policy Name	Key Features	Strengths	Limitations
HIPAA	Privacy rule; security rule; enforcement rule	Strong patient data protection; clear guidelines for healthcare providers	No specific regulations for AI; no accountability for AI algorithms
HITECH Act	Promotes EHR adoption; strengthens HIPAA enforcement	Encourages adoption and advancement of health IT; improved patient data security protections	Emphasis on advancing EHR adoption; does not fully apply to AI
21st Century Cures Act	Interoperability promotion; prohibition of information blocking	Quicker innovations; enhanced data sharing	Potential privacy concerns; no specific regulations and recommendations for interoperability with AI
GDPR	Data minimization; purpose limitation; right to be forgotten	Strong data protection; broadly applicable to many sectors	Complex and costly compliance requirements; strict regulations can create a roadblock for AI development and data access
AI Act	Decrease risk exposure to high-risk AI; enforcement and obligations for AI developers	Stricter AI regulation; decreased privacy and security risks; increased transparency	Potential increase in compliance costs that can trickle down to consumers

TABLE 1: Analysis of 5 existing digital health policies

AI = Artificial Intelligence, IT = Information Technology, HIPAA = Health Insurance Portability and Accountability Act, HITECH Act = The Health Information Technology for Economic and Clinical Health Act, GDPR = The General Data Protection Regulation.

[21-26]

With the plethora of global regulatory policies for healthcare data security and patient privacy already in place, it is critical to analyze the ability of those regulations to apply to AI in healthcare. There are many concerns regarding how these existing policies protect the privacy of patient data with large datasets being analyzed by AI algorithms. Major policies like HIPAA and GDPR provide a framework for protecting and managing patient data, but there is a significant need to address the challenges that are created with the use of AI algorithms to collect, sort, or analyze patient data. Furthermore, present and prospective opportunities encompass the integration of electronic health records among various health providers, the investment in health data science research, the generation of real-world data in a non-biased format including more diversity of collected data, the advancement of AI and robotics, and the promotion of public-private partnerships. Many ethical dilemmas and unforeseen repercussions arise from the implementation of any health information technology. To mitigate these issues, it is essential to establish regulatory frameworks governing the development, management, and procurement of AI and health information technology systems, foster public-private collaborations, and ensure the ethical and safe application of AI within the system to create a system based on science and trust [27].

A major priority for many countries around the world is improving the interoperability of artificial intelligence systems in healthcare while still upholding security standards that are used by the industry. The prospect of a more productive healthcare environment with improved quality of care is a prime reason for the rapid implementation of AI. However, regulations must achieve a balance that protects patient health information while allowing for innovation in the AI industry [28]. This remains difficult as it is largely ignored in many digital health policies.

Along with interoperability, many countries have issues with the transparency of certain policies when it comes to AI and the liability surrounding it in healthcare. Regulations about liability tend to be vague when it comes to AI systems' accountability, resulting in inconsistent case law [29]. This lack of transparency has the potential to lose the trust of healthcare professionals regarding AI-generated advice. With the AI ecosystem containing multiple parties involved, such as clinicians, healthcare systems, and manufacturers, it is vital that the consequences fall upon those who are actually liable. Physicians or healthcare systems face liability for malpractice and other negligence while the manufacturers or designers of the AI tool might face product liability. For example, if the physician interprets the AI output incorrectly, deviates from the standard of care, or uses it on the wrong patient group, the liability will fall on the clinician [29]. On the other hand, developers would be liable for injuries that resulted from errors in the product. The standards for healthcare software products have been inconsistent and have put more risk of liability on the physicians and healthcare systems [29]. In addition, with many AI algorithms lacking explainability, it is difficult for physicians to accurately assess the viability of the results produced by the algorithm, which further increases the difficulty in placing liability [30]. Many clinicians are not adequately trained, and patients are not adequately educated. However, liability falls on clinicians, while the outcome affects the patient. It is evident that the modern status quo is not a very equitable system and more efforts at educating each party should be done. There is much room for improvement regarding digital health policy and cybersecurity regulations, and it is critical that regulatory bodies dedicate extensive resources to create clear and adequate guidelines.

Cybersecurity risks for healthcare data

With examples of large-scale cybersecurity and technological systems in healthcare facing challenges due to cyberattacks or even simple updates that are caused by unintended bugs, lack of testing, and memory leaks, the healthcare system faces many challenges that threaten both the privacy and health of the patients. In the case of the 2024 cyberattack on Change Healthcare, which was likely due to a lack of multi-factor authentication, millions of health records and patient private health information were put at risk [31]. In addition to the attack costing Change Healthcare an estimated yearly cost of around 1.6 billion dollars, the disruption of the payment and claims processing due to the attack financially hurt various healthcare systems and individual practices around the US [32]. On the other hand, a simple software update in 2024 by CrowdStrike, a cybersecurity firm, led to a major disruption in healthcare systems amongst many other sectors by preventing Windows devices from working. As a result, health records were not able to be accessed, ID badges were not working, and emergency systems were down, which impacted both the practices and the health of the patients [33]. Current cybersecurity challenges in healthcare include protecting electronic health records, securing medical devices, and preventing ransomware attacks. Many countries around the world utilize electronic medical records, payment systems, and online communication, resulting in an increased threat of data leakage or theft. With the heavily digitized international healthcare industry today, advanced cybersecurity measures are needed to ensure the protection of patient data and the functionality of healthcare practices. As AI utilization increases in healthcare, the risk to patient data will only rise unless proper measures are put in place. On the other hand, utilization of AI in cybersecurity is not inherently bad as it can rapidly adapt to cyber threats. AI's role in cybersecurity assists in protecting patient data and creates a duality of purpose. In the future, finding the right balance and the best methods for AI usage will be essential for patient safety.

Cybersecurity implications of AI in healthcare

The implementation of AI in the US healthcare industry is projected to increase, with the AI market in healthcare predicted to have a compound annual growth rate of 44.2% between 2019 and 2027 [34]. With the rapid digitalization and implementation of AI in healthcare, many cybersecurity vulnerabilities have been introduced. With the large amount of patient data that AI systems have access to, serious cybersecurity risks of data breaches or leaks can arise [1]. As AI becomes more prevalent in the industry, a safeguard that organizations should implement is to minimize healthcare data exposure to AI systems, which can reduce the amount of patient data at risk in case of a data breach. However, since AI systems require extensive data access for algorithm training, developers and countries have to balance AI innovation with patient privacy in order to foster advances in the industry [28]. Given the recent cybersecurity events in healthcare that highlight the lack of proper cybersecurity checkpoints, AI handling of large amounts of data will only provide increased possibilities for hackers to detect vulnerabilities and gain exposure to sensitive medical information and patient records. An alternative that organizations can use is to allow AI systems to generate synthetic data for the training of its models. However, this, in turn, raises concerns about the diversity and effectiveness of the training itself. It is essential that organizations develop certain guidelines and standards that achieve a balance of both innovation and data security.

Artificial intelligence of things (AIoT) medical devices that use AI, such as smart health monitors and smartwatches, to collect and store patient health data in order to anticipate potential problems and needs. However, these devices have also been known to be vulnerable to security threats [2,13,35]. Cyberattacks and hackers can cause impaired device functionality in addition to leakage of health information and harm to the patient's health. On the other hand, Yamin et al highlighted that AI can be used on the offensive by breaching and manipulating medical records for financial, malicious, or political purposes [16]. AI can help cyberattackers adapt to detection systems by obtaining new data, thus allowing a potential evasion of security systems. This problem is particularly growing in importance as an official FBI notice warned about the threat of cyber criminals using AI in social engineering/phishing attacks by using artificially manipulated audio and visual content [36].

Impact of AI on health disparities

With the implementation of AI models into healthcare, it is becoming increasingly necessary to highlight the importance of diversity in AI. Especially with the sheer diversity in healthcare patient populations, it is imperative for AI systems to be trained in diversity and inclusion. If AI training does not include diversity, biases and lack of fairness could emerge during patient care which risks generalizability in AI healthcare decision-making [37,38]. With over half of the databases used to train AI-based models coming from the US or China, other populations who are not included in AI training are left at a disadvantage, thus amplifying healthcare disparities that were already present [37]. In addition to gathering data on different populations, datasets and studies need to be collected through various institutions in different regions to prevent the systemic bias of individual providers and healthcare systems from impacting the decision-making of the AI model [39]. Hence, it is necessary for AI companies to disclose how the models were trained to allow physicians and other clinicians to make accurate assessments of the applicability of the model in a certain patient population. Increased interpretability of AI models and training for healthcare providers will make identifying bias in algorithms easier [39]. Especially in cases with solo practice physicians in rural areas that serve minority communities, the understandability of the implicit biases that AI algorithms carry is necessary to prevent incorrect diagnoses and unnecessary costs to both the provider and patient. Eduard Fosch-Villaronga et al emphasizes the need for diversity in AI for medicine with the potential impact that algorithm bias may have on discrimination, safety, and privacy concerns for patients in increasing automated medicine. The current algorithm-based systems may lead to bias and, therefore, may provide misdiagnosis and miscalculations in racial minorities and marginalized communities [40]. They also highlighted that extending AI technologies that do not account for diversity risks unsafe and inadequate healthcare delivery. Development and implementation of AI algorithms in an inclusive diverse population will avoid exacerbations already existing in our system, and the formation of new prejudices [40]. Moreover, when using AI to guide studies, clinical trials, and treatment designs, it is essential to intentionally have diverse participants with respect to race, ethnicity, age, and gender to obtain inclusive and unbiased results [40]. In doing this, we have to ensure that all participants from different backgrounds are included in an appropriate number that is representative of their respective population proportions. Gender, sex, race, and ethnicity are used in AI algorithms in the healthcare context, research, and patient care; thus, they need to be leveraged to decrease bias and have more inclusive results. Consequently, interventions and solutions created by AI algorithms will be able to generalize to people of different races, ages, and genders, resulting in better overall outcomes.

Current landscape of healthcare cybersecurity

The United States and other western countries have been major players in the global healthcare cybersecurity market, with companies such as IBM, McAfee, Cisco Systems Inc., and Broadcom Inc. However, regions such as Asia will include some of the fastest-growing markets for healthcare cybersecurity with many countries having rapidly growing IT sectors and increased risk of security breaches in healthcare systems [41]. Countries like China, Japan, and India are making headway towards the digitization of healthcare [3]. As global healthcare reliance on technology and internet-based systems continues to grow, it is essential to promote collaboration between markets in different regions. As a result, preventable security breaches and challenges can be avoided while also enabling a venue for other regions to create their own sectors. Collaborative research and development initiatives can pave the way for innovation in cybersecurity solutions and allow for increased diversity in AI training algorithms.

True cost of cybersecurity

As global digitalization continues to increase, cybercrime is rapidly growing in prevalence around the world. Estimates have reported that cybersecurity threats cost the world roughly 6 trillion US dollars in 2021 [42,43]. This cybercrime cost is especially rising in healthcare, as cybercriminals use the confidential nature of healthcare data to gain ransom money from organizations or sell it to vendors. With over 42 million US patients being affected by cybercrime from 2016 to 2021 and the healthcare system in the US incurring a loss of 6 billion dollars in 2019, there is a growing need to invest in advanced cybersecurity measures [44,45]. Hence, it is critical for healthcare organizations to adhere to strict cybersecurity guidelines by conducting internal audits, prioritizing training programs, and innovating existing cybersecurity measures [45]. However, funding is a major issue for many organizations, hospital systems, and private entities, such as multi-specialty and solo practices, especially given the high cost for cybersecurity professionals, insurance policies, systems, and organization-wide training. Therefore, governments need to be involved and provide the necessary funds to protect patient data, provide funding for organizational implementation, and prevent any unnecessary financial losses due to cybercrime.

Recommendations

It is crucial for healthcare organizations and policymakers to address the issues that tag along with increased AI implementation in healthcare. The current legal framework and security structure are not enough to sufficiently address the various risks. As machine learning and AI algorithms collect and analyze personal data, there is an increased risk of security breaches [46]. With this increasing risk, more proactive strategies must take place to prevent significant jeopardization of patient data and safety. An effective strategy is to restrict AI to the least amount of patient data it needs to have adequate training and to make effective clinical decisions while also de-identifying the data in case of a data breach. However, while protecting patient privacy is a necessity, it is important not to apply too many restrictions that would lead to stunted innovation in the field or inadequate and ungeneralizable training of AI algorithms [47]. Other strategies could include creating real-time records of anyone interacting with patient records and requiring training of all staff in cybersecurity in hospital systems. With a majority of healthcare data breaches coming internally due to lack of training and negligence, employee training and education is a necessary and vital step toward protecting patient data [48]. By ensuring proper training and certification for all employees to reduce the risk of human-caused data leaks, healthcare systems can dedicate more resources toward advancing the cybersecurity of AI algorithms. Policymakers should clearly identify the liability across the various sectors to appropriately allocate responsibility when it comes to artificial intelligence [30]. Healthcare policies should be transparent and should not be shifting the majority of the burden on the physicians, but equally placing it amongst the various actors related to AI. This clarity fosters the appropriate application of AI and lessens the legal ambiguity (Table *2*).

Recommendations	Description	Potential Impact	Implementation Challenges
Require transparency with AI and other applications	Requiring AI developers to disclose the development of the algorithm, source codes, data inputs, and analytical approaches to its vendors or ethics committees.	Improved trust in AI systems in addition to easier assessments by hospital systems.	Private developers might not want the release of intellectual property. Potential government systems are a valid solution to this.
Government data protection standards and laws	Stricter data protection guidelines, such as access restrictions, will add another layer of safety for patient data.	Safer AI systems in hospital networks; ability to blacklist/fine AI systems that do not meet ethical requirements and pose a risk to patient safety.	Data protection authorities or AI developers might show some resistance.
Continuous AI system vulnerability assessments	Implement ongoing system monitoring and health checks that will identify any weaknesses or abnormalities.	Continuous system monitoring can determine and identify faults and prevent future breaches.	Can be very resource-intensive, and might need additional funding to properly implement.
AI ethics board requirement	Mandate that all hospital systems that use AI to a certain level must have an ethics committee.	This helps with answering any question regarding ethics in addition to adding another layer of protection to patient data.	Will require training for committee members in addition to additional funding.
AI-specific liability framework	Concrete standards meant to clearly appoint liability to certain parties in cases of AI system errors or breaches. Clear responsibility of burden of proof on a party for the situation.	This allows for most trust in AI in addition to a more just legal framework to appoint responsibility for certain faults.	Could be an initial challenge to properly define parameters for liability.
Mandatory AI cybersecurity training and awareness programs	Require cybersecurity training for all healthcare staff to specifically teach about the security risks of AI.	Improved awareness of security risks will help protect the whole hospital system from any breaches caused by individuals.	This method would be very resource-intensive, and might have to be merged with other training modules.

TABLE 2: Recommendations for AI Implementation into Healthcare.

AI=Artificial Intelligence

[49-50]

Additionally, rules should encourage the sharing of knowledge about cybersecurity threats and best practices across healthcare companies. In the healthcare industry, cooperation and knowledge sharing can strengthen the group’s security against cyberattacks [51]. The sharing of data, such as healthcare charges, can allow easier detection of fraud, which further saves costs [52,53]. Moreover, frameworks such as the one launched by the US National Institute of Standards and Technology, which promotes a collaboration between the US government and private entities to improve cybersecurity, are a necessary step towards protecting patient data. Collaboration would allow the sharing of resources and strategies to optimize cybersecurity and also improve patient and physician trust in the technology, which would in turn benefit the healthcare system as a whole due to its lack of resources in IT [48]. Another method to promote the sharing of knowledge is the consolidation of healthcare insurance companies. This can be seen in countries with single-payer or multi-payer universal healthcare, which allows for consolidation of health insurance into a single unit or multiple providers respectively [53,54]. In addition to saving in administration costs through consolidation of billing, fewer insurance payouts, and the price negotiation, the single-payer model of insurance will allow better care for the population through increased access and economical clinical services and administrative costs. By allowing easier access to healthcare screenings and prevention programs, the long-term costs can be lessened by reducing incidences of diseases [53,54]. Single-payer systems are usually controlled by the government which regulates healthcare spending through government funds. However, complete consolidation could lead to potential monopolistic control of the market if the single-payer misuses the power. There is no correct answer to this dilemma as different countries have varying situations. This is seen with many countries that provide universal healthcare choosing a more complex and costly multi-payer system that also involves private entities, which in turn increases competition for innovation [53,55]. Nevertheless, consolidation and collaboration to some degree in health insurance will benefit through sharing information about both cybersecurity and healthcare indicators, which will allow for more innovation and advancement of the industry [53,54]. Finally, in order to maintain patient safety and trust, we need a diverse AI algorithm development that is accounts for race, ethnicity, gender, and age. Diverse patient populations that are used in AI training increased ability for AI guidance to be safely applicable to a diverse range of people.

Conclusions

With the evolving nature of the healthcare industry, more advanced technologies and forms of artificial intelligence will continue to make their impact. However, many cybersecurity risks will emerge with the increased implementation of new technologies and AI models. Thus, governments must take the initiative to pass health policies that factor in this new wave of advancement. Healthcare organizations also need to be proactive in promoting employee awareness in addition to developing strategies to prevent any serious issues and protect sensitive patient data. It is also important to establish clear liability parameters for defining the responsibility in case of adverse cybersecurity outcomes caused due to AI integration. As artificial intelligence continues to integrate into healthcare, inclusivity in AI training and data collection by incorporating diverse populations in algorithm training should be of importance to both the providers and developers to allow for adequate generalization to diverse patient populations. In order to foster patient education and safety, developers and companies should maintain transparency of AI algorithm training and tendencies to the providers. This will allow clinicians to make accurate assessments and better assist patients in making more informed decisions. With the growing prevalence of AI and digital innovation in healthcare, the importance of cybersecurity should take precedence to improve the safety of patient data, accuracy and diversity of data, implications in patient care of a diverse population, and the trust of patients, physicians, and all healthcare workers in the system. Integrating the results will lead to increased access, enhanced quality, and equity of care as well as reducing the cost of care.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Deepkumar Patel, Karen Allison, Abdullah Virk, Safanah Alasmari

Acquisition, analysis, or interpretation of data: Deepkumar Patel, Karen Allison, Abdullah Virk, Safanah Alasmari

Drafting of the manuscript: Deepkumar Patel, Karen Allison, Abdullah Virk, Safanah Alasmari

Critical review of the manuscript for important intellectual content: Deepkumar Patel, Karen Allison, Abdullah Virk, Safanah Alasmari

Supervision: Deepkumar Patel, Karen Allison, Abdullah Virk

Disclosures

Conflicts of interest: In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

References

1. Alowais SA, Alghamdi SS, Alsuhebany N, et al.: Revolutionizing healthcare: the role of artificial intelligence

in clinical practice. BMC Med Educ. 2023, 23:689. 10.1186/s12909-023-04698-z

2. Giansanti D: Cybersecurity and the digital-Health: the challenge of this millennium . Healthcare (Basel). 2021, 9:62. 10.3390/healthcare9010062
3. Thomason J: Big tech, big data and the new world of digital health . Glob Health J. 2021, 5:165-8. 10.1016/j.glohj.2021.11.003
4. Jones LD, Golan D, Hanna SA, Ramachandran M: Artificial intelligence, machine learning and the evolution of healthcare: A bright future or cause for concern?. Bone Joint Res. 2018, 7:223-5. 10.1302/2046-3758.73.BJR-2017-0147.R1
5. Mahesh N, Devishamani CS, Raghu K, Mahalingam M, Bysani P, Chakravarthy AV, Raman R: Advancing healthcare: the role and impact of AI and foundation models. Am J Transl Res. 2024, 16:2166-79. 10.62347/WQWV9220
6. Rodríguez-Ruiz A, Krupinski E, Mordang JJ, Schilling K, Heywang-Köbrunner SH, Sechopoulos I, Mann RM: Detection of breast cancer with mammography: effect of an artificial intelligence support system . Radiology. 2019, 290:305-14. 10.1148/radiol.2018181371
7. Shafi S, Parwani AV: Artificial intelligence in diagnostic pathology . Diagn Pathol. 2023, 18:109. 10.1186/s13000-023-01375-z
8. Malkani AL, Roche MW, Kolisek FR, et al.: Manipulation under anesthesia rates in technology-assisted versus conventional-instrumentation total knee arthroplasty. Surg Technol Int. 2020, 36:336-40.
9. Ofa SA, Ross BJ, Flick TR, Patel AH, Sherman WF: Robotic total knee arthroplasty vs conventional total knee arthroplasty: a nationwide database study. Arthroplast Today. 2020, 6:1001-8.e3. 10.1016/j.artd.2020.09.014
10. Nwoye E, Woo WL, Gao B, Anyanwu T: Artificial intelligence for emerging technology in surgery: systematic review and validation. IEEE Rev Biomed Eng. 2023, 16:241-59. 10.1109/RBME.2022.3183852
11. Soufyane A, Abdelhakim BA, Ahmed MB: An intelligent chatbot using NLP and TF-IDF algorithm for text understanding applied to the medical field. Emerging Trends in ICT Sustainable Development. Springer International Publishing, 2021. 3-10. 10.1007/978-3-030-53440-0_1
12. Laymouna M, Ma Y, Lessard D, Schuster T, Engler K, Lebouché B: Roles, users, benefits, and limitations of chatbots in health care: rapid review. J Med Internet Res. 2024, 26:e56930. 10.2196/56930
13. Junaid SB, Imam AA, Balogun AO, et al.: Recent advancements in emerging technologies for healthcare management systems: a survey. Healthcare (Basel). 2022, 10:1940. 10.3390/healthcare10101940
14. Quazi S: Artificial intelligence and machine learning in precision and genomic medicine . Med Oncol. 2022, 39:120. 10.1007/s12032-022-01711-1
15. Basu K, Sinha R, Ong A, Basu T: Artificial intelligence: how is it changing medical sciences and its future? . Indian J Dermatol. 2020, 65:365-70. 10.4103/ijd.IJD_421_20
16. Yamin MM, Ullah M, Ullah H, Katt B: Weaponized AI for cyber attacks. J Inf Secur Appl. 2021, 57:102722. 10.1016/j.jisa.2020.102722
17. Kaur R, Gabrijelčič D, Klobučar T: Artificial intelligence for cybersecurity: literature review and future research directions. Inf Fusion. 2023, 97:101804. 10.1016/j.inffus.2023.101804
18. Essén A, Stern AD, Haase CB, et al.: Health app policy: international comparison of nine countries' approaches. NPJ Digit Med. 2022, 5:31. 10.1038/s41746-022-00573-1
19. Murdoch B: Privacy and artificial intelligence: challenges for protecting health information in a new era . BMC Med Ethics. 2021, 22:122. 10.1186/s12910-021-00687-3
20. Meszaros J, Minari J, Huys I: The future regulation of artificial intelligence systems in healthcare services and medical research in the European Union. Front Genet. 2022, 13:927721. 10.3389/fgene.2022.927721
21. 21st century Cures act . (2020). Accessed: August 29, 2024: https://www.fda.gov/regulatory-information/selected-amendments-fdc-act/21st-century-cures-act.
22. AI act. (2025). Accessed: February 20, 2025: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.
23. General data protection regulation (GDPR) - legal text . (2018). Accessed: February 20, 2025: https://gdpr-info.eu/.
24. HIPAA and your health rights . (2021). Accessed: August 29, 2024: https://www.hhs.gov/programs/hipaa/index.html.
25. HITECH act enforcement interim final rule. (2017). Accessed: August 29, 2024: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.
26. Sarpatwari A, Kesselheim AS: The 21st century cures act: opportunities and challenges . Clin Pharmacol Ther. 2015, 98:575-7. 10.1002/cpt.208
27. Sheikh A, Anderson M, Albala S, et al.: Health information technology and digital innovation for national learning health and care systems. Lancet Digit Health. 2021, 3:383-96. 10.1016/S2589-7500(21)00005-4
28. Bak M, Madai VI, Fritzsche MC, Mayrhofer MT, McLennan S: You can't have AI both ways: balancing health data privacy and access fairly. Front Genet. 2022, 13:929453. 10.3389/fgene.2022.929453
29. Maliha G, Gerke S, Cohen IG, Parikh RB: Artificial intelligence and liability in medicine: balancing safety and innovation. Milbank Q. 2021, 99:629-47. 10.1111/1468-0009.12504
30. Cestonaro C, Delicati A, Marcante B, Caenazzo L, Tozzo P: Defining medical liability when artificial intelligence is applied on diagnostic algorithms: a systematic review. Front Med (Lausanne). 2023, 10:1305756. 10.3389/fmed.2023.1305756
31. Change healthcare cyberattack was due to a lack of multifactor authentication, UnitedHealth CEO says . (2024). Accessed: February 20, 2025: https://apnews.com/article/change-healthcare-cyberattack-unitedhealth-senate-9e2fff70ce4f93566043210bdd347a1f.
32. UnitedHealth to take up to $1.6 billion hit this year from Change hack . (2024). Accessed: February 20, 2025: https://www.reuters.com/business/healthcare-pharmaceuticals/unitedhealth-warns-115-135share-hit-this-year-hack-2024-0....
33. The Crowdstrike outage disrupted many industries. Hospitals were especially vulnerable . (2024). Accessed: February 20, 2025: https://www.npr.org/2024/07/21/nx-s1-5046700/the-crowdstrike-outage-disrupted-many-industries-hospitals-were-especial....

34. Dicuonzo G, Donofrio F, Fusco A, Shini M: Healthcare system: moving forward with artificial intelligence . Technovation. 2023, 120:102510. 10.1016/j.technovation.2022.102510
35. Pise AA, Almuzaini KK, Ahanger TA, Farouk A, Pant K, Pareek PK, Nuagah SJ: Enabling artificial intelligence of things (AIoT) healthcare architectures and listing security issues. Comput Intell Neurosci. 2022, 2022:8421434. 10.1155/2022/8421434
36. FBI warns of increasing threat of cyber criminals utilizing artificial intelligence . (2024). Accessed: February 20, 2025: https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-util....
37. Celi LA, Cellini J, Charpignon ML, et al.: Sources of bias in artificial intelligence that perpetuate healthcare disparities: a global review. PLOS Digit Health. 2022, 1:e0000022. 10.1371/journal.pdig.0000022
38. Shams RA, Zowghi D, Bano M: AI and the quest for diversity and inclusion: a systematic literature review . AI Ethics. 2023, 5:411-38. 10.1007/s43681-023-00362-w
39. Moore CM: The challenges of health inequities and AI . Intelligence-based Med. 2022, 6:100067. 10.1016/j.ibmed.2022.100067
40. Fosch-Villaronga E, Drukarch H, Khanna P, Verhoef T, Custers B: Accounting for diversity in AI for medicine. Comput Law Secur Rev. 2022, 47:105735. 10.1016/j.clsr.2022.105735
41. Kandasamy K, Srinivas S, Achuthan K, Rangan VP: Digital healthcare - cyberattacks in asian organizations: an analysis of vulnerabilities, risk, NIST perspectives, and recommendations. IEEE. 2022, 10:12345-64. 10.1109/ACCESS.2022.3145372
42. The 2020 official annual cybercrime report . (2020). Accessed: February 20, 2025: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/.
43. Williams CM, Chaturvedi R, Chakravarthy K: Cybersecurity risks in a pandemic . J Med Internet Res. 2020, 22:e23692. 10.2196/23692
44. Kessler SR, Pindek S, Kleinman G, Andel SA, Spector PE: Information security climate and the assessment of information security risk among healthcare employees. Health Informatics J. 2020, 26:461-73. 10.1177/1460458219832048
45. Alanazi AT: Clinicians' perspectives on healthcare cybersecurity and cyber threats . Cureus. 2023, 15:e47026. 10.7759/cureus.47026
46. Shaw J, Rudzicz F, Jamieson T, Goldfarb A: Artificial Intelligence and the implementation challenge. J Med Internet Res. 2019, 21:e13659. 10.2196/13659
47. Price WN 2nd, Cohen IG: Privacy in the age of medical big data . Nat Med. 2019, 25:37-43. 10.1038/s41591-018-0272-7
48. Ghafur S, Grass E, Jennings NR, Darzi A: The challenges of cybersecurity in health care: the UK national health service as a case study. Lancet Digit Health. 2019, 1:10-2. 10.1016/S2589-7500(19)30005-6
49. Artificial intelligence and cybersecurity in healthcare (YEL2023) . (2023). Accessed: February 20, 2025: https://ihf-fih.org/news-insights/artificial-intelligence-and-cybersecurity-in-healthcare/ .
50. Ethics and governance of artificial intelligence for health: guidance on large multi-modal models . (2024). Accessed: August 30, 2024: https://iris.who.int/bitstream/handle/10665/375579/9789240084759-eng.pdf.
51. Cohen IG, Evgeniou T, Gerke S, Minssen T: The European artificial intelligence strategy: implications and challenges for digital health. Lancet Digit Health. 2020, 2:376-9. 10.1016/S2589-7500(20)30112-6
52. Lu JF, Hsiao WC: Does universal health insurance make health care unaffordable? Lessons from Taiwan . Health Aff (Millwood). 2003, 22:77-88. 10.1377/hlthaff.22.3.77
53. Petrou P, Samoutis G, Lionis C: Single-payer or a multipayer health system: a systematic literature review . Public Health. 2018, 163:141-52. 10.1016/j.puhe.2018.07.006
54. Galvani AP, Parpia AS, Foster EM, Singer BH, Fitzpatrick MC: Improving the prognosis of health care in the USA. Lancet. 2020, 395:524-33. 10.1016/S0140-6736(19)33019-3
55. Hussey P, Anderson GF: A comparison of single- and multi-payer health insurance systems and options for reform. Health Policy. 2003, 66:215-28. 10.1016/S0168-8510(03)00050-2