GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(Review Article)

Advancements in health information technology and their role in enhancing cancer care: Innovations in early detection, treatment, and data privacy

Amir Mohammad Karimi Forood [1,*], Adegboyega Daniel Osifuwa [2], Joy Ene Idoko [2], Oyebola Oni [2], Comfort Seun Ajaelu [2] and Francis Agbo Idoko [3]

[1] *Department of Biomedical Engineering, University of Connecticut, Storrs, CT, USA.*
[2] *Department of Biomedical Engineering, University of Ibadan, Ibadan, Nigeria.*
[3] *Department of Fisheries Technology, Bauchi State College of Agriculture, Bauchi, Nigeria.*

GSC Advanced Research and Reviews, 2024, 21(01), 228–241

Publication history: Received on 08 September 2024; revised on 15 October 2024; accepted on 17 October 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.21.1.0380

Abstract

The rapid advancement of Health Information Technology (HIT) has revolutionized cancer care, introducing new capabilities in early detection, individualized treatment, and data security. This paper reviews the key HIT innovations that have reshaped oncology, including the widespread adoption of Electronic Health Records (EHRs), the use of artificial intelligence (AI) in diagnostic processes, and the application of telemedicine and predictive analytics to improve treatment planning. These technologies have enabled earlier and more accurate diagnoses, expanded access to care, and facilitated data-driven, personalized treatment strategies. In parallel, this review addresses the importance of safeguarding sensitive patient data, focusing on encryption, anonymization techniques, and the regulatory frameworks like HIPAA and GDPR that ensure data privacy. Finally, the paper discusses future directions for HIT, particularly the potential of AI-driven decision support systems, real-time data analytics, and privacy-enhancing algorithms to further advance cancer care, creating a more secure, efficient, and patient-centered healthcare system.

Keywords: Health Information Technology (HIT); Cancer Care; Personalized Cancer Treatment; AI in Cancer Diagnosis; Genomic Data in Cancer Treatment; Patient Data Security

1. Introduction

Health Information Technology (HIT) has become a driving force in the transformation of cancer care, impacting areas such as diagnostic accuracy, personalized treatments, and overall care delivery. The adoption of electronic health records (EHRs) has streamlined patient management, improving coordination among healthcare providers and enhancing patient safety [1]. Innovations in artificial intelligence (AI) and machine learning (ML) have contributed to earlier detection of cancer, reduced diagnostic errors, and improved clinical decision-making by enabling more precise data analysis [1,2]. Moreover, AI and ML tools support personalized treatment approaches by analyzing genetic and molecular data to recommend therapies tailored to the individual patient. In oncology, this approach—often referred to as precision medicine—has been revolutionary. By integrating genomic data into HIT systems, healthcare providers can better predict how a patient will respond to certain treatments, enabling more precise, targeted therapies. This not only improves treatment efficacy but also minimizes adverse effects, allowing for a more patient-centered approach to cancer care [3].

The introduction of telemedicine and remote monitoring tools has allowed continuous care for patients, especially those undergoing cancer treatment, expanding access to healthcare in ways previously unattainable [2,4]. Despite these

---

[*] Corresponding author: Amir Mohammad Karimi Forood

advances, significant challenges remain in protecting patient data. Regulations such as HIPAA and GDPR play a vital role in ensuring data privacy and secure management, which are critical in safeguarding sensitive patient information [5].

This review aims to explore the innovations in HIT that have dramatically improved cancer care, with a focus on three key areas: early detection, treatment personalization, and data privacy. By analyzing the latest technological developments and their implementation, this paper will provide a comprehensive overview of how HIT is reshaping the landscape of oncology. Furthermore, it will discuss the future potential of HIT to enhance cancer care, particularly through the continued evolution of AI, machine learning, and real-time data analytics, as well as the ongoing challenges of ensuring robust data security and privacy.

2. Innovations in Early Detection and Diagnosis

The integration of artificial intelligence (AI), machine learning (ML), and digital imaging technologies has transformed early-stage cancer detection, leading to higher diagnostic accuracy and better patient outcomes. These advancements enable healthcare providers to analyze vast datasets, extract meaningful patterns, and make predictions that surpass human capabilities. AI and ML have not only improved early detection but have also reduced diagnostic errors, resulting in more timely interventions and optimized treatment planning.

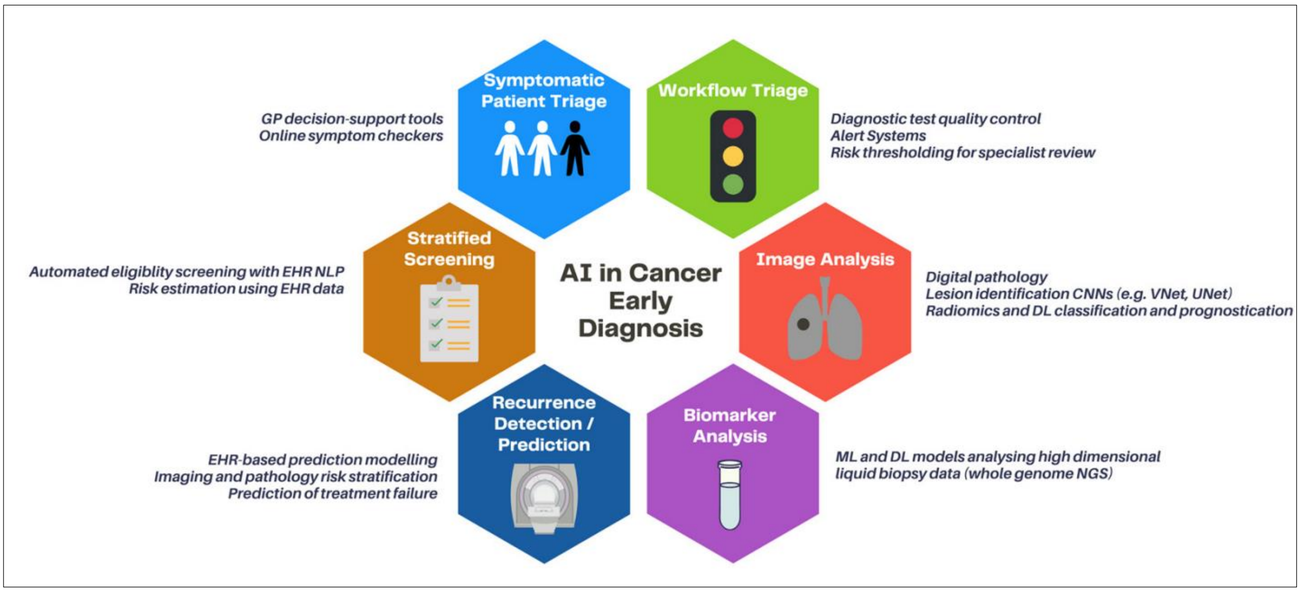

Figure 1 Clinical Applications of Artificial Intelligence (AI) in Early Cancer Diagnosis: Integration of Natural Language Processing (NLP), Machine Learning (ML), Deep Learning (DL), and Next-Generation Sequencing (NGS) with Electronic Health Records (EHRs) to Assist General Practitioners (GPs) [6].

2.1. AI and Machine Learning in Cancer Screening

AI algorithms, particularly deep learning, have been widely applied in various cancer detection methods. For instance, deep learning-based image analysis has been used to detect lung cancer in computed tomography (CT) scans. In many cases, AI-driven tools have outperformed radiologists by identifying subtle patterns that might otherwise go unnoticed [6–8]. In breast cancer screening, AI systems analyzing mammograms have demonstrated an improved ability to detect microcalcifications and other early signs of malignancy, achieving higher accuracy than traditional methods [9,10]. These AI systems have significantly reduced false-positive and false-negative rates, ultimately leading to better patient outcomes.

Another notable application of AI in cancer detection is its use in liquid biopsies. These non-invasive techniques, when combined with machine learning models, analyze circulating tumor DNA (ctDNA) to predict the presence of early-stage cancers. AI-based models have shown great promise in enhancing the sensitivity and specificity of these biopsies, making it possible to detect cancer even when only trace amounts of ctDNA are present in the bloodstream [11].

2.2. Digital Imaging Technologies in Early Detection

Digital imaging technologies, such as optical imaging and ultrasound, are being increasingly integrated with AI to further improve early cancer detection. For example, ultrasound imaging, traditionally used for breast cancer detection, has seen significant improvements through the application of AI algorithms. These systems can automatically segment and classify tumor tissues, thereby providing more accurate and faster diagnoses [2, 6]. Optical imaging technologies are also being employed in the detection of skin, oral, and cervical cancers, offering non-invasive and cost-effective solutions in low-resource settings [12,13].

In regions with limited access to high-end diagnostic equipment, AI-enhanced thermography has been employed as a supplementary screening tool for breast cancer. This technology leverages thermal imaging combined with machine learning models to detect anomalies in breast tissue, providing a non-invasive, radiation-free alternative to mammography in resource-limited areas [14].

2.3. Summary of Innovations

Table 1 provides a concise overview of key innovations in artificial intelligence (AI), machine learning (ML), and digital imaging technologies that are revolutionizing early cancer detection. By summarizing these advancements, the table helps readers distinguish the different pathways through which these technologies are enhancing diagnostic accuracy, improving patient outcomes, and expanding access to care. Understanding these innovations is crucial for grasping the impact they have on reducing diagnostic errors and enabling earlier interventions, particularly in resource-limited settings where traditional diagnostic tools may be less accessible.

Table 1 Summary of Key AI, Machine Learning, and Digital Imaging Innovations in Early Cancer Detection

Technology	**Application**	**Example Innovation**
AI in Lung Cancer Detection	CT Scan Analysis	AI algorithms outperform radiologists in detecting early-stage lung cancer by identifying subtle patterns in CT scans [6–8].
AI in Breast Cancer Screening	Mammogram Analysis	AI systems improve detection of microcalcifications, reducing false-positive and false-negative results in mammography [9,10].
ML in Liquid Biopsy	Circulating Tumor DNA (ctDNA) Analysis	ML models enhance sensitivity and specificity of liquid biopsies, detecting trace amounts of ctDNA for early diagnosis [15].
Digital Imaging in Breast Cancer	Ultrasound Imaging	AI enhances the segmentation and classification of tumor tissues in breast cancer detection using ultrasound [8,9].
Optical Imaging for Skin and Cervical Cancer	Non-invasive Detection in Low-Resource Settings	Optical imaging combined with AI detects early-stage skin and cervical cancers in low-resource settings [12,13].
AI-Enhanced Thermography	Breast Cancer Screening	AI models analyze thermal imaging for non-invasive, radiation-free breast cancer screening in resource-limited areas [14].

These advancements in AI, ML, and digital imaging are transforming early cancer detection, making it more efficient and accessible across diverse healthcare settings. As these technologies continue to evolve, they hold immense potential to reduce cancer mortality rates by enabling earlier interventions, especially in low-resource environments.

3. Electronic Health Records (EHRs) in Risk Assessment and Screening

Electronic health records (EHRs) have become essential tools in modern healthcare for managing patient data, facilitating clinical decision-making, and improving overall care. EHRs play a significant role in streamlining risk assessment and screening by providing centralized access to patient histories, risk factors, and clinical decision support systems (CDSS). The integration of these systems has made it easier for healthcare providers to identify patients at risk for various conditions, ensuring that appropriate screening measures are taken.

EHRs have enabled the development of sophisticated risk assessment models that use patient data to predict the likelihood of diseases such as cancer, cardiovascular conditions, and infections. By incorporating social determinants of health (SDOH), family history, and genetic information, EHRs can provide personalized risk scores and suggest preventive interventions [16,17].

However, the use of EHRs also comes with challenges. Data security risks, privacy concerns, and system usability are major issues that need addressing to ensure that these systems provide maximum benefit without compromising patient safety or confidentiality. Hospitals and clinics have implemented cybersecurity measures such as encryption and multifactor authentication to protect sensitive patient data [18,19]. Furthermore, EHR safety guidelines, such as the SAFER guides, help institutions maintain system safety and reliability [20].

EHRs also enable better clinical research by providing large datasets that can be mined to generate new insights and predictive models. This feature is invaluable for developing evidence-based practices and improving patient outcomes [21,22].

Through understanding the advantages and disadvantages of incorporating Electronic Health Records (EHRs) into risk assessment and screening processes, scholars can gain a deeper comprehension of how these systems are revolutionizing contemporary healthcare. Table 2 enumerates the salient characteristics of EHR integration, emphasizing their contribution to improved clinical decision-making, better patient data access, and individualized risk prediction models. Simultaneously, it tackles obstacles such potential threats to data security and the intricacy of incorporating social determinants of health (SDOH). This synopsis aids in emphasizing the advantages and disadvantages of EHRs for enhancing screening precision and assisting with extensive healthcare projects.

Table 2 Overview of Benefits and Drawbacks of EHR Integration in Risk Assessment and Screening

Feature	**Benefits**	**Drawbacks**
Clinical Decision Support for Risk Assessment	EHRs support automated risk assessments for conditions like hyperbilirubinemia, streamlining clinical decisions [23].	Risk prediction models are not always accurate, and false positives may lead to unnecessary interventions [16,17].
Centralized Access to Patient Data [24,25]	EHRs enable access to comprehensive patient histories and risk factors, improving screening accuracy.	Incomplete or outdated records may lead to incorrect risk assessments or missed screening opportunities.
Social Determinants of Health (SDOH) Inclusion [16,17,26]	EHRs incorporate SDOH, improving risk assessment by considering external factors affecting health outcomes.	Integration of SDOH into EHRs is complex and may introduce biases in risk prediction models.
EHRs in Screening Programs [27,28]	EHRs have been used in large-scale screening efforts, such as hepatitis C screening in integrated health systems.	Implementing and managing screening programs through EHRs requires significant training and financial investment.
Cybersecurity Measures for EHRs [18,19,29]	Strong cybersecurity measures protect sensitive data, ensuring patient privacy and compliance with regulations.	Cybersecurity threats, such as data breaches, remain a significant concern in EHR management.
Support for Clinical Research [21,22,25,26]	EHRs provide vast datasets for research, aiding in the development of risk prediction models and clinical studies.	Data quality and consistency issues can affect the reliability of research findings derived from EHR data.

4. Technological Advancements in Cancer Treatment

Health Information Technology (HIT) has revolutionized precision medicine, genetic profiling, and personalized cancer treatment by enabling more accurate and individualized care. The use of genetic data in electronic health records (EHRs) is a key component of this transformation. Genetic profiling allows clinicians to identify specific mutations that may influence treatment responses and risk factors. For instance, the integration of BRCA1/2 mutation information into EHRs helps guide the use of targeted therapies such as PARP inhibitors, which are more effective for patients with these specific mutations [30].

The adoption of clinical decision support systems (CDSS) further enhances personalized cancer treatment by utilizing patient-specific genetic and molecular data to recommend individualized therapies. CDSS have become indispensable in oncology, where they help oncologists make informed decisions about complex treatment regimens. This approach not only increases the effectiveness of treatments but also reduces side effects by tailoring therapies to the patient's genetic makeup [31]. As such, the incorporation of genetic profiling into HIT systems has allowed for a more refined approach to cancer care, ensuring that patients receive the most appropriate and personalized treatments [32].

HIT also plays a critical role in precision medicine initiatives that rely on vast datasets. These systems enable clinicians and researchers to manage and analyze genetic, clinical, and therapeutic data at an unprecedented scale. The ability to link genetic data with clinical outcomes allows for real-time adjustments to treatment plans based on a patient's response, creating a more dynamic and adaptable care process [33]. Additionally, the development of oncology informatics has provided a robust framework for integrating diverse types of data, which supports personalized treatment strategies across various cancer types [2].

EHRs that include genetic information are not only useful for treatment but also for risk prediction. For example, genetic testing integrated into HIT systems allows clinicians to assess the risk of hereditary cancers, enabling early intervention through screening and preventive measures such as prophylactic surgery [34]. The identification of patients at higher risk of certain cancers, based on genetic predisposition, supports the proactive management of their health, leading to improved outcomes [35].

Moreover, HIT has supported personalized cancer treatment by improving communication between patients and providers. The use of patient portals and mobile technologies, connected to EHRs, empowers patients to access their genetic and clinical information, enhancing patient engagement in their own care [36]. Patients are increasingly able to participate in decisions regarding their treatment options, particularly when they are informed about their genetic risk factors and treatment pathways [37].

Despite these advances, the integration of genetic data into HIT systems comes with challenges, particularly regarding data privacy and security. Managing the ethical and logistical concerns of storing and sharing sensitive genetic information is critical. There is a pressing need to develop stronger data protection measures to ensure that patients' genetic information is not misused [38]. Moreover, the interoperability of HIT systems remains a challenge, as the seamless exchange of genetic data across different platforms and institutions is essential for maximizing the potential of personalized medicine [39].

In conclusion, HIT has significantly advanced the field of precision medicine, particularly in oncology, by facilitating genetic profiling, enhancing risk prediction, and supporting personalized treatment plans. The continued evolution of HIT systems promises further improvements in cancer care, enabling more effective, individualized therapies based on genetic insights and patient-specific data.

Telemedicine has emerged as a transformative force in healthcare, significantly altering how patients and healthcare providers interact. Its rise is particularly notable in the context of cancer care and treatment planning, where timely and accessible care is critical. The use of telemedicine has expanded rapidly, driven by advancements in digital health technologies, the increasing availability of high-speed internet, and the need for remote care solutions during the COVID-19 pandemic [40,41]. Telemedicine platforms allow healthcare providers to consult with patients remotely, monitor their progress, and adjust treatment plans in real-time, ensuring continuous care regardless of geographical barriers [42]. This has been especially beneficial for cancer patients, who often require ongoing management and monitoring over extended periods.

In addition to improving access to care, telemedicine has been complemented by the rise of predictive analytics, which uses machine learning and artificial intelligence (AI) to forecast patient outcomes and optimize treatment planning. Predictive analytics leverages vast amounts of data, including patient medical history, genetic information, and real-time monitoring data from wearable devices, to predict disease progression and response to therapies [43,44]. This technology has allowed oncologists to develop personalized treatment plans that are more precise and tailored to the individual needs of patients.

Telemedicine's integration with predictive analytics enhances its value by providing healthcare providers with tools to anticipate potential complications or treatment failures. For instance, predictive models can be used to identify patients who are at high risk of treatment-related side effects, allowing for early interventions to mitigate these risks. By utilizing deep data analytics, clinicians can refine treatment protocols, monitor patient progress remotely, and adjust care plans based on predictive insights [44]. The application of predictive analytics in telemedicine also supports proactive health management, helping patients avoid emergency interventions through timely adjustments to their treatment plans [45,46].

Telemedicine platforms, when combined with AI-driven predictive analytics, have created a robust framework for continuous patient care. The ability to deliver personalized, data-driven care remotely has improved patient outcomes and increased the efficiency of healthcare systems. This combination of telemedicine and predictive analytics has paved the way for a more integrated, patient-centric approach to cancer care, allowing for real-time decision-making and personalized treatment adjustments that significantly enhance the patient experience [45,46].

The future of telemedicine and predictive analytics in treatment planning looks promising, with ongoing innovations in AI, machine learning, and data analytics expected to further enhance the capabilities of these technologies. As healthcare systems continue to embrace digital health solutions, telemedicine and predictive analytics will likely play an even greater role in delivering personalized, high-quality care to patients across the globe.

5. Data Privacy and Security Challenges in Cancer Care

The protection of sensitive cancer patient data is critical in the era of digital health technologies, where large volumes of personal health information are routinely collected, stored, and shared across various platforms. With the increasing reliance on electronic health records (EHRs), mobile health applications, and genomic databases, safeguarding patient privacy has become a primary concern for healthcare providers and technology developers alike [47,48]. The nature of cancer treatment requires extensive data collection, including genomic information, treatment histories, and ongoing health monitoring, which creates unique challenges in ensuring data security [49,50].

One of the most pressing concerns in this domain is the need to balance the benefits of data sharing for research and treatment optimization with the imperative to protect patient privacy. For instance, platforms like UPCARE have been developed to facilitate user privacy-preserving cancer research by using encryption and privacy-preserving protocols that allow researchers to collaborate without compromising sensitive patient information [51]. However, the integration of artificial intelligence (AI) and big data analytics in healthcare complicates the matter further, as these technologies often require access to vast amounts of data, raising concerns about unauthorized access, data breaches, and ethical use [47,52].

The challenges posed by digital health technologies in protecting patient data are multifaceted. Cybersecurity risks, including hacking, phishing, and ransomware attacks, are constant threats to healthcare systems. As more healthcare services migrate to cloud-based platforms and telemedicine, the attack surface for cybercriminals expands, exposing patient data to increased risk [53,54]. Mobile health platforms, in particular, have been highlighted as vulnerable to security breaches, with insufficient encryption and inadequate user authentication protocols being common issues [55].

Data privacy concerns are further exacerbated by the global nature of cancer research. Cross-institutional data sharing, especially in international collaborations, increases the complexity of ensuring consistent privacy standards across different legal frameworks and regulations [56]. For example, the European General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. provide strict guidelines on data protection, but the implementation of these regulations varies across institutions, making it challenging to maintain a unified standard of patient privacy protection [57].

Moreover, genomic data presents its own set of privacy challenges. Unlike other forms of medical data, genomic information is inherently identifiable and can reveal information not only about the individual but also about their family members. Protecting genomic data in cancer research is therefore a critical ethical concern. Advanced encryption techniques and genomic data privacy frameworks have been proposed to address these concerns, but these solutions are not yet universally adopted [48,58].

Ethical considerations also play a significant role in the discussion of data protection in cancer care. Patients must be fully informed about how their data will be used and consent to its collection and sharing. However, achieving informed consent in the digital age is challenging, particularly when dealing with complex technologies like AI and machine learning that may be difficult for patients to fully understand [59]. Ensuring transparency and maintaining patient trust is therefore crucial in the deployment of digital health technologies.

In conclusion, protecting sensitive cancer patient data is of paramount importance in the age of digital health technologies. While the benefits of digital innovation in cancer care are undeniable, including improved treatment outcomes and more efficient research collaborations, these advancements also bring significant challenges in data privacy and security. Addressing these challenges will require ongoing efforts in cybersecurity, ethical governance, and international collaboration to ensure that patient data remains secure and that the trust between patients and healthcare providers is upheld. Here's a table that illustrates the progression in protecting sensitive cancer patient data and the challenges posed by digital health technologies over time, using key references from the provided list:

Table 3 Progression of Cancer Patient Data Protection and Challenges Posed by Digital Health Technologies Over Time

Time Period	**Progress in Protecting Cancer Patient Data**	**Challenges Posed by Digital Health Technologies**
Early 2000s [54,56]	- Introduction of basic Electronic Health Records (EHRs) to store patient data securely.	- Limited security measures in EHRs, increasing vulnerability to data breaches.
Mid 2000s [56,60]	- Data encryption techniques introduced for protecting patient records in healthcare.	- Lack of standardization in data protection across institutions, complicating cross-institutional sharing.
2010s [55,57]	- Enhanced regulatory frameworks such as GDPR (Europe) and HIPAA (US) for patient data privacy.	- Growth of mobile health platforms with inadequate security protocols (e.g., weak encryption, poor user authentication).
Early 2020s [47,51,53]	- Adoption of privacy-preserving platforms (e.g., UPCARE) for cancer research to allow secure data sharing.	- Increased cybersecurity threats, such as ransomware and phishing attacks, as healthcare services move online.
Mid 2020s [47,52,59]	- Integration of AI and big data analytics for enhanced data protection and cancer research.	- Difficulty ensuring patient consent and transparency in AI-driven platforms, due to the complexity of the technology.
Future Outlook [48,57,58]	- Advanced cryptographic techniques for genomic data protection in cancer research.	- Challenges in ensuring global data privacy standardization as more institutions collaborate internationally.

Table 3 shows a clear progression from basic EHRs and encryption techniques in the early 2000s to more sophisticated privacy-preserving platforms and AI-driven solutions in the 2020s, alongside the evolving challenges posed by digital health technologies.

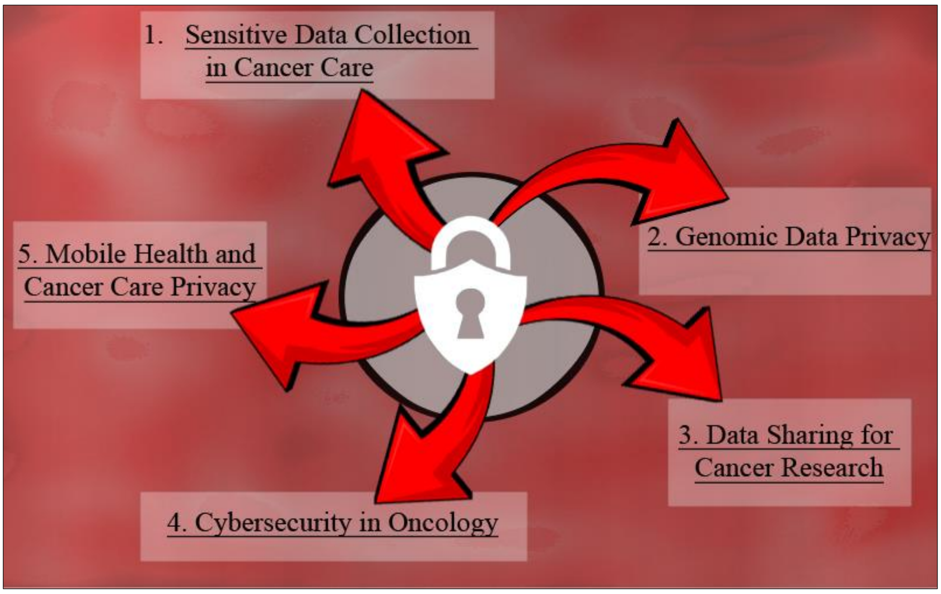

Figure 2 Key data privacy challenges in cancer care. In a technologically advanced healthcare setting, protecting personal health data—including genetic and treatment data—is crucial to promoting safe, efficient, and moral cancer care.

5.1. Advancements in data encryption, anonymization, and the regulatory framework supporting data security

As the healthcare sector becomes more reliant on digital technologies, safeguarding sensitive patient information, particularly cancer patient data, has become a critical concern. Data encryption, anonymization techniques, and robust regulatory frameworks are pivotal in protecting this sensitive information from breaches and unauthorized access.

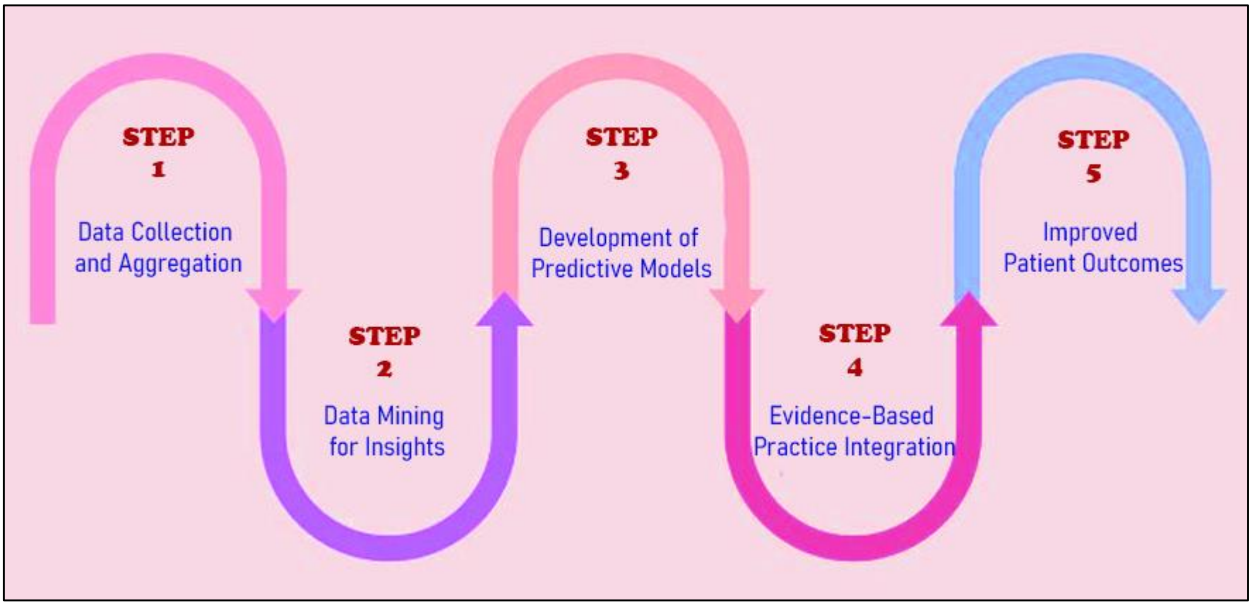

Figure 3 Managing EHR Data as a Path to Unlock Predictive Insights and Improve Patient Care

Understanding the process of Electronic Health Records (EHR) data management is vital for fully leveraging its advantages in clinical research and healthcare improvement. Figure 3 illustrates the step-by-step progression from data collection to achieving better patient outcomes using EHR data. This systematic approach is important because it ensures that data is carefully processed, analysed, and applied to generate insights that directly influence patient care and clinical decisions.

5.2. Data Encryption Advancements

Encryption plays a fundamental role in protecting patient data by converting sensitive information into an unreadable format, which can only be decrypted by authorized users. The Advanced Encryption Standard (AES) has emerged as one of the most widely used encryption algorithms, providing robust security for data in healthcare systems. AES outperforms older methods, such as the Data Encryption Standard (DES), by offering stronger encryption and faster processing speeds, making it ideal for handling large datasets, including those found in cancer patient records [61]. More recent advancements include homomorphic encryption, which allows data to be encrypted while still being processed, enabling secure data analysis without compromising privacy. This method is especially promising for privacy-preserving cancer research and other sensitive health applications [62,63].

Encryption techniques are being further refined to address the specific challenges of cloud storage and data transmission in telemedicine and mobile health platforms. As more healthcare services move online, encryption has become essential in securing patient data during transmission, storage, and access. For instance, smart systems and Internet of Things (IoT) devices used in healthcare increasingly rely on cloud-based storage solutions, where encrypted data can be securely offloaded and processed remotely [64]. This is critical for ensuring the privacy of cancer patients' medical records in cloud environments, where traditional security measures may fall short [65].

5.3. Anonymization Techniques

Anonymization, another crucial technique, removes personally identifiable information from datasets, enabling the use of medical data for research without compromising patient privacy. Recent advances in clustering-based anonymization techniques have shown significant promise in preserving data privacy while maintaining data utility. These methods organize data into clusters, ensuring that individual patient records cannot be re-identified [66]. Anonymization is particularly important for sharing cancer research data across institutions, where maintaining patient confidentiality is paramount.

However, achieving effective anonymization in the age of big data is a growing challenge. Data anonymization faces difficulties, especially when working with genomic data, where even anonymized data can sometimes be re-identified due to the uniqueness of genetic information [67,68]. To address these concerns, sophisticated techniques such as differential privacy are being developed, which introduce controlled statistical noise to the data, preserving privacy while allowing for meaningful analysis [69]. This is especially relevant in cancer research, where large-scale data sharing is necessary for progress but must be balanced against the risk of compromising patient privacy.

5.4. Regulatory Frameworks Supporting Data Security

The implementation of robust regulatory frameworks, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe, has provided essential guidance for protecting sensitive healthcare data. HIPAA, enacted in 1996, was one of the first regulations to establish national standards for electronic healthcare transactions, requiring healthcare providers to implement measures like encryption and anonymization to protect patient information [70]. Similarly, GDPR, which came into force in 2018, sets strict guidelines for data privacy and security, ensuring that personal health information is handled with care and that patients are informed about how their data is used and stored [71,72].

These regulatory frameworks not only govern the protection of personal health information but also facilitate the ethical sharing of data for research purposes. For instance, in cancer genomics research, GDPR and HIPAA provide clear protocols for obtaining patient consent and ensuring that data is adequately anonymized before it is shared across institutions [71,73]. The increasing use of AI and big data in healthcare has raised new concerns about compliance, prompting updates to these frameworks to address issues like automated decision-making and data sovereignty [74].

Despite these advancements, challenges remain in ensuring that data privacy laws keep pace with technological innovation. In many developing countries, regulatory frameworks for protecting sensitive healthcare data are still evolving, creating gaps in patient data security when cross-border data sharing occurs [75]. Therefore, ongoing efforts to harmonize data privacy standards across different jurisdictions are crucial to maintaining the integrity of international cancer research collaborations.

Table 4 Key Data Privacy Technologies and Their Associated Challenges in Safeguarding Cancer Patient Information

Advancement/Technology	Description	Challenges
Advanced Encryption Standard (AES) [61,65,76]	AES is widely used for encrypting healthcare data, offering robust security and fast performance compared to older standards like DES.	Increased processing time for very large datasets; not immune to emerging cryptographic attacks.
Homomorphic Encryption [8,63,65]	Allows encrypted data to be processed without decryption, preserving privacy during analysis.	Computationally intensive and not yet widely adopted for large-scale healthcare data applications.
Clustering-Based Anonymization [66,69]	Organizes patient data into clusters, preserving privacy while maintaining the utility of data for research.	Difficulties in maintaining data utility, especially for large and diverse cancer datasets.
Differential Privacy [67–69]	Adds statistical noise to datasets, ensuring that individual patient information is protected while allowing analysis.	May reduce the accuracy of data analysis, especially in small datasets or highly detailed genomic data.
HIPAA (Health Insurance Portability and Accountability Act) [70,73,74]	A U.S. regulatory framework that mandates standards for protecting electronic health information.	Challenges in adapting HIPAA to cover emerging technologies such as AI and telemedicine platforms.

GDPR (General Data Protection Regulation) [71,72,75]	European regulation providing strict data privacy and protection laws, including healthcare data.	Compliance across borders can be complex, especially with international collaborations in cancer research.
Data Protection in Genomic Research [67,68,71]	Requires advanced anonymization and encryption techniques to protect highly identifiable genetic information.	Genomic data can often be re-identified, posing a risk to patient privacy in cancer research.

6. Conclusion

Health Information Technology (HIT) has significantly transformed cancer care by enhancing early detection, supporting personalized treatment plans, and safeguarding sensitive patient data. Key contributions of HIT to cancer care include the integration of Electronic Health Records (EHRs), which streamline patient data management and enable seamless access to clinical information, improving coordination between healthcare providers. The use of predictive analytics and AI-driven diagnostics has led to earlier detection of cancers, with more accurate predictions of disease progression and outcomes. Additionally, personalized medicine is now more feasible, thanks to the integration of genetic and molecular data into patient care, allowing for more targeted therapies based on individual patient profiles.

Looking ahead, technological innovations such as homomorphic encryption, privacy-preserving algorithms, and further developments in AI and machine learning promise to revolutionize cancer care even further. These innovations will enhance the ability to process and share sensitive patient data securely across institutions, enabling more collaborative research while maintaining patient privacy. The future of cancer care will likely see a greater reliance on real-time data analytics and AI-driven treatment recommendations, improving the precision of cancer therapies and facilitating earlier interventions. These advancements will drive more effective, data-driven, and patient-centered care, paving the way for global collaborations that can tackle cancer more efficiently.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflicts of interest.

Statement of ethical approval.

The authors state that the research was conducted according to ethical standards.

References

[1] El-Kareh R, Hasan O, Schiff GD. Use of health information technology to reduce diagnostic errors. BMJ Qual Saf. 2013 Oct 1;22(Suppl 2):ii40–51.

[2] Tarver WL, Menachemi N. The impact of health information technology on cancer care across the continuum: a systematic review and meta-analysis. J Am Med Inform Assoc. 2016 Mar 1;23(2):420–7.

[3] Miriovsky BJ, Shulman LN, Abernethy AP. Importance of Health Information Technology, Electronic Health Records, and Continuously Aggregating Data to Comparative Effectiveness Research and Learning Health Care. J Clin Oncol. 2012 Dec 1;30(34):4243–8.

[4] Clauser SB, Wagner EH, Aiello Bowles EJ, Tuzzio L, Greene SM. Improving Modern Cancer Care Through Information Technology. Am J Prev Med. 2011 May 1;40(5, Supplement 2):S198–207.

[5] Singh H, Sittig DF. Measuring and improving patient safety through health information technology: The Health IT Safety Framework. BMJ Qual Saf. 2016;25(4):226–32.

[6] Hunter B, Hindocha S, Lee RW. The role of artificial intelligence in early cancer diagnosis. Cancers. 2022;14(6):1524.

[7] Rai HM. Cancer detection and segmentation using machine learning and deep learning techniques: a review. Multimed Tools Appl. 2023 Aug 22;83(9):27001–35.

[8] Painuli D, Bhardwaj S. Recent advancement in cancer diagnosis using machine learning and deep learning techniques: A comprehensive review. Comput Biol Med. 2022;146:105580.

[9] Guo R, Lu G, Qin B, Fei B. Ultrasound imaging technologies for breast cancer detection and management: a review. Ultrasound Med Biol. 2018;44(1):37–70.

[10] Yue W, Wang Z, Chen H, Payne A, Liu X. Machine learning with applications in breast cancer diagnosis and prognosis. Designs. 2018;2(2):13.

[11] Karimi Forood AM. Mechanisms of telomere dysfunction in cancer from genomic instability to therapy: A review. Int J Sci Res Arch. 2024 Sep 17;13:806–14.

[12] Hou H, Mitbander R, Tang Y, Azimuddin A, Carns J, Schwarz RA, et al. Optical imaging technologies for in vivo cancer detection in low-resource settings. Curr Opin Biomed Eng. 2023;100495.

[13] Bedard N, Pierce M, El-Naggar A, Anandasabapathy S, Gillenwater A, Richards-Kortum R. Emerging Roles for Multimodal Optical Imaging in Early Cancer Detection: A Global Challenge. Technol Cancer Res Treat. 2010 Apr;9(2):211–7.

[14] Dar RA, Rasool M, Assad A. Breast cancer detection using deep learning: Datasets, methods, and challenges ahead. Comput Biol Med. 2022;149:106073.

[15] Liu L, Chen X, Petinrin OO, Zhang W, Rahaman S, Tang ZR, et al. Machine learning protocols in early cancer detection based on liquid biopsy: a survey. Life. 2021;11(7):638.

[16] Chen M, Tan X, Padman R. Social determinants of health in electronic health records and their impact on analysis and risk prediction: a systematic review. J Am Med Inform Assoc. 2020;27(11):1764–73.

[17] Goldstein BA, Navar AM, Pencina MJ, Ioannidis JP. Opportunities and challenges in developing risk prediction models with electronic health records data: a systematic review. J Am Med Inform Assoc JAMIA. 2017;24(1):198.

[18] Sandhane R, Patil K, Sharma AR. Cyber Security Risk Assessment for Electronic Medical Records (EMRs). In: 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) [Internet]. IEEE; 2024 [cited 2024 Sep 27]. p. 1–6. Available from: https://ieeexplore.ieee.org/abstract/document/10563486/

[19] Alarfaj KA, Rahman MH. The Risk Assessment of the Security of Electronic Health Records Using Risk Matrix. Appl Sci. 2024;14(13):5785.

[20] Sittig DF, Sengstack P, Singh H. Guidelines for US hospitals and clinicians on assessment of electronic health record safety using SAFER guides. JAMA. 2022;327(8):719–20.

[21] Cowie MR, Blomster JI, Curtis LH, Duclaux S, Ford I, Fritz F, et al. Electronic health records to facilitate clinical research. Clin Res Cardiol. 2017 Jan;106(1):1–9.

[22] Yadav P, Steinbach M, Kumar V, Simon G. Mining Electronic Health Records (EHRs): A Survey. ACM Comput Surv. 2018 Nov 30;50(6):1–40.

[23] Petersen JD, Lozovatsky M, Markovic D, Duncan R, Zheng S, Shamsian A, et al. Clinical decision support for hyperbilirubinemia risk assessment in the electronic health record. Acad Pediatr. 2020;20(6):857–62.

[24] Menachemi N, Collum. Benefits and drawbacks of electronic health record systems. Risk Manag Healthc Policy. 2011 May;47.

[25] Kondru VLP. Electronic Health Care Records-Boon To Industry. Int J Med Inform AI. 2015;2(2):1–18.

[26] Coorevits P, Sundgren M, Klein GO, Bahr A, Claerhout B, Daniel C, et al. Electronic health records: new opportunities for clinical research. J Intern Med. 2013 Dec;274(6):547–60.

[27] Geboy AG, Nichols WL, Fernandez SJ, Desale S, Basch P, Fishbein DA. Leveraging the electronic health record to eliminate hepatitis C: Screening in a large integrated healthcare system. PLoS One. 2019;14(5):e0216459.

[28] Silow-Carroll S, Edwards JN, Rodin D. Using electronic health records to improve quality and efficiency: the experiences of leading hospitals. Issue Brief Commonw Fund. 2012;17(1):40.

[29] Kruse CS, Smith B, Vanderlinden H, Nealand A. Security Techniques for the Electronic Health Records. J Med Syst. 2017 Aug;41(8):127.

[30] Ritchie JB, Allen CG, Morrison H, Nichols M, Lauzon SD, Schiffman JD, et al. Utilization of health information technology among cancer genetic counselors. Mol Genet Genomic Med. 2020 Aug;8(8):e1315.

[31] Bouaud J, Blaszka-Jaulerry B, Zelek L, Spano JP, Lefranc JP, Cojean-Zelek I, et al. Health information technology: use it well, or don't! Findings from the use of a decision support system for breast cancer management. In: AMIA Annual Symposium Proceedings [Internet]. American Medical Informatics Association; 2014 [cited 2024 Sep 27]. p. 315. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4419891/

[32] Scott S, Abul-Husn N, Owusu Obeng A, Sanderson S, Gottesman O. Implementation and utilization of genetic testing in personalized medicine. Pharmacogenomics Pers Med. 2014 Aug;227.

[33] Hesse BW, Arora NK, Klein WM. Communication science: connecting systems for health. In: Hesse BW, Ahern D, Beckjord E, editors. Oncology Informatics: Using Health Information Technology to Improve Processes and Outcomes in Cancer Care. Boston, MA: Elsevier Inc; 2016. p. 253-275.

[34] Nguyen TV, Eisman JA. Genetic profiling and individualized assessment of fracture risk. Nat Rev Endocrinol. 2013;9(3):153–61.

[35] Rogowski W. Genetic screening by DNA technology: a systematic review of health economic evidence. Int J Technol Assess Health Care. 2006;22(3):327–37.

[36] Klasnja P, Hartzler A, Powell C, Pratt W. Supporting cancer patients' unanchored health information management with mobile technology. In: AMIA Annual Symposium Proceedings [Internet]. American Medical Informatics Association; 2011 [cited 2024 Sep 27]. p. 732. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3243297/

[37] Lee JL, Rawl SM, Dickinson S, Teal E, Baker LB, Lyu C, et al. Communication About Health Information Technology Use Between Patients and Providers. J Gen Intern Med. 2020 Sep;35(9):2614–20.

[38] Shoenbill K, Fost N, Tachinardi U, Mendonca EA. Genetic data and electronic health records: a discussion of ethical, logistical and technological considerations. J Am Med Inform Assoc. 2014;21(1):171–80.

[39] Nardi EA, Lentz LK, Winckworth-Prejsnar K, Abernethy AP, Carlson RW. Emerging issues and opportunities in health information technology. J Natl Compr Canc Netw. 2016;14(10):1226–33.

[40] Khan S, Khan B. The Rise Of Telemedicine: Transforming Healthcare Delivery. Open Horiz Sci Rev. 2023;1(02):11–9.

[41] Losorelli SD, Vendra V, Hildrew DM, Woodson EA, Brenner MJ, Sirjani DB. The Future of Telemedicine: Revolutionizing Health Care or Flash in the Pan? Otolaryngol Neck Surg. 2021 Aug;165(2):239–43.

[42] Nandan M, Mitra S, Parai A, Jain R, Agrawal M, Singh U. Telemedicine (e-Health, m-Health). Des Intell Healthc Syst Prod Serv Using Disruptive Technol Health Inform. 2022;1.

[43] Sachdeva S, Ali A. Rise of Telemedicine in Healthcare Systems Using Machine Learning: A Key Discussion. In: Sharma K, Gigras Y, Sharma V, Hemanth DJ, Poonia RC, editors. Internet of Healthcare Things [Internet]. 1st ed. Wiley; 2022. p. 113–30. Available from: https://onlinelibrary.wiley.com/doi/10.1002/9781119792468.ch6

[44] Bhatia M, Hooda M, Gupta P. Deep Data Analytics: Future of Telehealth. In: Research Anthology on Telemedicine Efficacy, Adoption, and Impact on Healthcare Delivery [Internet]. IGI Global; 2021 [cited 2024 Sep 27]. p. 274–95. Available from: https://www.igi-global.com/chapter/deep-data-analytics/273470

[45] Kumari N, Banerjee M. Telemedicine: A New Horizon in Public Health Management. In: Leveraging the Potential of Artificial Intelligence in the Real World [Internet]. CRC Press; 2025 [cited 2024 Sep 27]. p. 1–20.

[46] Ekvitayavetchanukul P, Bhavani C, Nath N, Sharma L, Aggarwal G, Singh R. Revolutionizing Healthcare: Telemedicine and Remote Diagnostics in the Era of Digital Health. In: Kumar P, Singh P, Diwakar M, Garg D, editors. Healthcare Industry Assessment: Analyzing Risks, Security, and Reliability. Cham: Springer; 2024. p. 255-77. (Engineering Cyber-Physical Systems and Critical Infrastructures; vol. 11).

[47] Yee TM, Raj K. The Dual Challenge of Enhancing Healthcare Delivery and Protecting Patient Privacy in the Age of Advanced Artificial Intelligence Technologies. J Hum Behav Soc Sci. 2022;6(7):63–72.

[48] Mohammed Yakubu A, Chen YPP. Ensuring privacy and security of genomic data and functionalities. Brief Bioinform. 2020;21(2):511–26.

[49] Siu LL, Lawler M, Haussler D, Knoppers BM, Lewin J, Vis DJ, et al. Facilitating a culture of responsible and effective sharing of cancer genome data. Nat Med. 2016;22(5):464–71.

[50] Vyas A, Abimannan S, Hwang R. Sensitive Healthcare Data: Privacy and Security Issues and Proposed Solutions. In: Mangla M, Sharma N, Mittal P, Wadhwa VM, Thirunavukkarasu K, Khan S, editors. Emerging Technologies for

Healthcare [Internet]. 1st ed. Wiley; 2021 [cited 2024 Sep 27]. p. 93–127. Available from: https://onlinelibrary.wiley.com/doi/10.1002/9781119792345.ch4

[51] Bramm G, Önen M, Schanzenbach M, Komarov I, Morgner F, Tiebel C, Cadavid J. UPCARE: User Privacy-preserving Cancer Research Platform. In: SECRYPT 2024, 21st International Conference on Security and Cryptography; 2024 Jul; Dijon, France.

[52] Thapa C, Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy. Comput Biol Med. 2021;129:104130.

[53] Duckert M, Barkhuus L. Protecting Personal Health Data through Privacy Awareness: A study of perceived data privacy among people with chronic or long-term illness. Proc ACM Hum-Comput Interact. 2022 Jan 14;6(GROUP):1–22.

[54] Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egypt Inform J. 2021;22(2):177–83.

[55] Harvey MJ, Harvey MG. Privacy and security issues for mobile health platforms. J Assoc Inf Sci Technol. 2014 Jul;65(7):1305–18.

[56] Van der Haak M, Wolff AC, Brandner R, Drings P, Wannenmacher M, Wetter T. Data security and protection in cross-institutional electronic patient records. Int J Med Inf. 2003;70(2–3):117–30.

[57] Andersen MR, Storm HH. Cancer registration, public health and the reform of the European data protection framework: abandoning or improving European public health research? Eur J Cancer. 2015;51(9):1028–38.

[58] Hashmi B, Khan R. Cybersecurity Protocols in Medical Engineering: Safeguarding Advanced Cancer Treatment Technologies. J Environ Sci Technol. 2024 Jan 10;3(1):302–22.

[59] Adekunle Oyeyemi Adeniyi, Jeremiah Olawumi Arowoogun, Chioma Anthonia Okolo, Rawlings Chidi, Oloruntoba Babawarun. Ethical considerations in healthcare IT: A review of data privacy and patient consent issues. World J Adv Res Rev. 2024 Feb 28;21(2):1660–8.

[60] Gostin L. Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations. Ann Intern Med. 1997 Oct 15;127(8_Part_2):683.

[61] Kasiran Z, Ali HF, Noor NM. Time performance analysis of advanced encryption standard and data encryption standard in data security transaction. Indones J Electr Eng Comput Sci. 2019;16(2):988.

[62] Aguilar-Melchor C, Fau S, Fontaine C, Gogniat G, Sirdey R. Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain. IEEE Signal Process Mag. 2013;30(2):108–17.

[63] Qureshi MB, Qureshi MS, Tahir S, Anwar A, Hussain S, Uddin M, et al. Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud. Symmetry. 2022;14(4):695.

[64] Gudimetla SR. Data Encryption in Cloud Storage. Int Res J Mod Eng Technol Sci. 2024;6:2582–5208.

[65] Du G. Advancements in Encryption Techniques for Enhancing Meteorological Data Security During Catastrophic Weather Events. J Prog Eng Phys Sci. 2023;2(4):26–36.

[66] Majeed A, Khan S, Hwang SO. Toward privacy preservation using clustering based anonymization: recent advances and future research outlook. IEEE Access. 2022;10:53066–97.

[67] Vokinger KN, Stekhoven DJ, Krauthammer M. Lost in Anonymization — A Data Anonymization Reference Classification Merging Legal and Technical Considerations. J Law Med Ethics. 2020;48(1):228–31.

[68] Neves F, Souza R, Sousa J, Bonfim M, Garcia V. Data privacy in the Internet of Things based on anonymization: A review. J Comput Secur. 2023;31(3):261–91.

[69] Salas J, Domingo-Ferrer J. Some Basics on Privacy Techniques, Anonymization and their Big Data Challenges. Math Comput Sci. 2018 Sep;12(3):263–74.

[70] Manion FJ, Robbins RJ, Weems WA, Crowley RS. Security and privacy requirements for a multi-institutional cancer research data grid: an interview-based study. BMC Med Inform Decis Mak. 2009 Dec;9(1):31.

[71] Scheibner J, Ienca M, Kechagia S, Troncoso-Pastoriza JR, Raisaro JL, Hubaux JP, et al. Data protection and ethics requirements for multisite research with health data: a comparative examination of legislative governance frameworks and the role of data protection technologies. J Law Biosci. 2020;7(1):lsaa010.

[72] Yeng PK, Fauzi MA, Sun L, Yang B. Assessing the legal aspects of information security requirements for health care in 3 countries: Scoping review and framework development. JMIR Hum Factors. 2022;9(2):e30050.

[73] Siu LL, Lawler M, Haussler D, Knoppers BM, Lewin J, Vis DJ, et al. Facilitating a culture of responsible and effective sharing of cancer genome data. Nat Med. 2016;22(5):464–71.

[74] Dove ES, Phillips M. Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective. In: Gkoulalas-Divanis A, Loukides G, editors. Medical Data Privacy Handbook [Internet]. Cham: Springer International Publishing; 2015 [cited 2024 Sep 27]. p. 639–78. Available from: https://link.springer.com/10.1007/978-3-319-23633-9_24

[75] Atadoga A, Farayola OA, Ayinla BS, Amoo OO, Abrahams TO, Osasona F. A comparative review of data encryption methods in the USA and Europe. Comput Sci IT Res J. 2024;5(2):447–60.

[76] Saini JK, Saini K. New Advance Encryption Standard to Analyze Encrypted Image Quality. Int J Comput Appl. 2013;74(7):1–5.