Journal of Digital Health
https://ojs.luminescience.cn/JDH

LUMINESCIENCE
https://luminescience.cn/

Review Article

Enhancing patient autonomy in data ownership: privacy models and consent frameworks for healthcare

Minal R. Narkhede *, **Nilesh I. Wankhede**, **Akanksha M. Kamble**

SMBT College of Pharmacy, Nashik, Maharashtra 422403, India

*Correspondence: Minal R. Narkhede, smbt_pharmaceutics@rediffmail.com

Abstract: Patient autonomy in healthcare has become increasingly significant in the digital age as individuals seek greater control over their health data. This review examines the ethical, legal and technological aspects of patient data ownership, emphasizing the need for privacy models and consent frameworks to empower patients, safeguard privacy and enhance transparency. Traditional doctor-patient confidentiality faces challenges due to advancements such as electronic health records, artificial intelligence and wearable technologies, necessitating updated frameworks to protect patient rights. Privacy models such as private, public and hybrid models present varying implications for data control, security and societal benefits. Emerging technologies such as blockchain and AI are revolutionizing data privacy by decentralizing data storage and enabling patient control while ensuring secure and ethical data utilization. Advanced consent frameworks, including dynamic and granular consent, provide patients with flexibility and transparency and promote trust and active participation in data-sharing decisions. Real-world implementations, such as Australia's My Health Record and Estonia's e-Health system, demonstrate the potential of patient-centric privacy frameworks to enhance healthcare quality and innovation. However, significant challenges persist, including regulatory ambiguities, cybersecurity risks and gaps in digital literacy. Addressing these issues requires collaboration among stakeholders to develop adaptable, secure and interoperable systems that prioritize patient autonomy. By integrating patient education, fostering interoperability and leveraging adaptive technologies, healthcare systems can balance privacy and innovation, build trust and ensure ethical data practices that empower individuals while advancing public health objectives.

Keywords: Patient autonomy, Data ownership, Privacy models, Consent frameworks, Blockchain, Artificial intelligence

Received: Dec.10, 2024; Revised: Feb.3, 2025; Accepted: Feb.10, 2025, Published: Mar.3, 2025

DOI: https://doi.org/10.55976/jdh.4202513361-23

1. Introduction

Patient autonomy is a foundational principle of healthcare ethics that emphasizes the individual's right to make informed decisions about their health [1] and personal information [2]. With the increasing integration of digital technologies in healthcare, the concept of data ownership has become a central component of patient autonomy. This shift underscores the belief that patients should have the authority to control their health data and determine who can access, share or use it [3]. Maintaining this level of autonomy not only protects human's rights, but also strengthens the patient-physician relationship and increases patients' roles and responsibilities. The increased use of technologies such as electronic health record (EHR), artificial intelligence (AI) diagnostics and wearable health technologies has also changed healthcare by making it more flexible and enabling personalized interventions. However, this technological transformation also brings significant ethical challenges related to data privacy, security and the extent of control patients have over their own health information [4]. In the past, patient information was protected through doctor-patient confidentiality, but with the digitization of health data, the boundaries are becoming increasingly blurred [5]. Patients often do not know exactly how their data may be shared, used or stored beyond their immediate care settings, which may potentially undermine their autonomy. The rapid pace of digital healthcare innovation requires a comprehensive frameworks to address these concerns and maintain transparency and ethical use of data [6]. Patient autonomy, in the context of data ownership, becomes crucial in ensuring that patients can actively participate in decisions regarding their health information. Privacy models that define how health data is accessed and utilized within the healthcare ecosystem, are essential for protecting patients' rights. These models provide mechanisms to safeguard sensitive information from misuse or unauthorized access and ensure that patient data is used in accordance with strict ethical guidelines [7].

Consent frameworks are equally important as they offer patients the opportunity to give informed consent about how their data is used. By ensuring that patients are fully informed about who can access their data and for what purpose [8], these frameworks allow individuals to retain control over their personal health information [9]. Together, privacy models and consent frameworks form a robust system to protect patient autonomy in the digital healthcare landscape. When implemented properly, they foster trust, encourage patient engagement and uphold ethical standards that prioritize the rights of patients. As healthcare systems become more digitized, the ownership and management of health data will continue to raise complex ethical issues. Ensuring that patients have control over their data not only supports their autonomy but also empowers them to make better-informed decisions about their healthcare [10]. It also helps to establish a patient-centered healthcare system that prioritizes privacy, security and ethical data usage. Moreover, these frameworks have the potential to advance clinical research, innovation and precision medicine by ensuring that patient data is shared in a way that respects autonomy while contributing to broader healthcare goals. The importance of establishing clear frameworks for data ownership, particularly as digital health technologies evolve, cannot be overemphasized [11]. These frameworks must be flexible enough to adapt to new developments and ensure that patient autonomy remains central in an increasingly complex digital healthcare environment. Ultimately, respecting for patient autonomy in the context of data ownership enhances not only the rights of individuals but also the overall quality and effectiveness of healthcare delivery. The growing importance of patient data ownership in healthcare is underscored by a mix of ethical, legal and practical challenges, especially in an era of increasing digital technologies and widespread data sharing. From an ethical perspective, patient autonomy is a core principle that enables individuals to make informed decisions about their own health and the data that pertains to it [12]. The ability to control access to one's health data is integral to preserving this autonomy, with concerns about exploitation by third parties for commercial purposes or targeting vulnerable populations without consent being central to the debate [13].

Legally, frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the US and the General Data Protection Regulation (GDPR) in Europe regulate data protection and privacy, but fail to address the core issue of data ownership [14]. This leaves open the question of whether patients really "own" their data, or whether ownership is shared with or claimed by healthcare providers, institutions or even governments. The ambiguity about the legal ownership of patient data complicates the development of consistent regulations that can safeguard patients' rights while enabling the proper use of data in medical research and innovation. Practically, managing the vast amounts of patient data in healthcare systems is a significant operational challenge [15]. Healthcare organizations must ensure transparency in data handling and obtain informed consent from patients. This is becoming increasingly complex as digital tools such as EHR and AI-driven data analysis technologies are integrated into healthcare systems [16]. In light of these ethical, legal and practical considerations, emerging technologies such as electronic consent (eConsent) systems are reshaping the way healthcare practices deal with patients' rights and privacy on their data [17]. These systems aim to improve the way in which patients are informed and empowered to make decisions regarding their health data, ensuring that autonomy is respected while also addressing the operational and legal complexities associated with data use [18].

This review highlights the importance of patients' ownership frameworks of their data in healthcare, which emphasizes and also balances privacy and consent frameworks to safeguard patients' autonomy and the use of digital technologies in healthcare. Models of data ownership such as private, public and hybrid models offer varying levels of control and usage rights. Privacy models such as HIPAA and GDPR address security but lack clarity on ownership. Other tools such as EHRs, AI and wearables improve care, but also raise concerns about data privacy and control. Emerging consent models, such as dynamic and granular consent, empower patients to manage data sharing and modify permissions. Technologies such as blockchain and AI enhance privacy, decentralization and patient control. Case studies from different countries demonstrate real-world applications and highlight the importance of adaptable frameworks to balance autonomy, innovation and ethical data use in digital healthcare.

2. The concept of data ownership in healthcare

The concept of data ownership in healthcare is a complex and evolving issue, influenced by various legal, ethical and technological factors. At the heart of this discussion is the question: Who owns patient data? There are three main models of data ownership in healthcare, as shown in Figure 1.

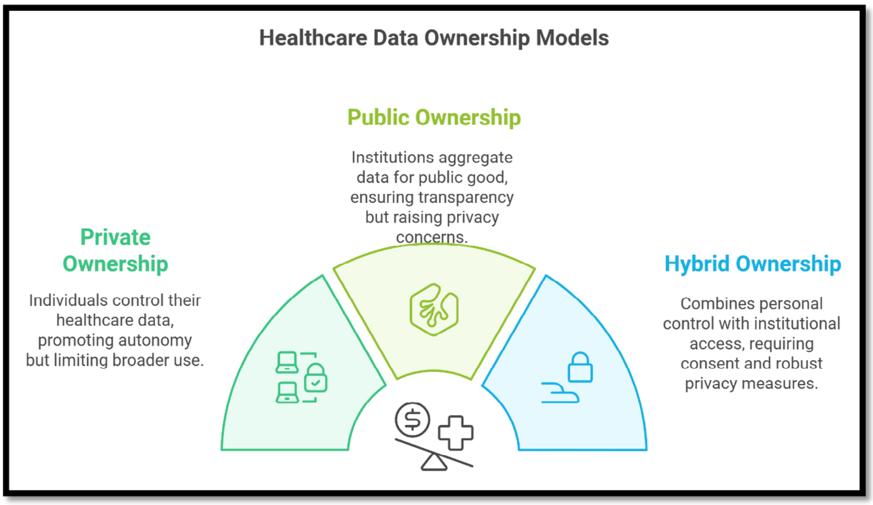
Healthcare Data Ownership Models
Public Ownership
Institutions aggregate data for public good, ensuring transparency but raising privacy concerns.
Private Ownership
Individuals control their healthcare data, promoting autonomy but limiting broader use.
Hybrid Ownership
Combines personal control with institutional access, requiring consent and robust privacy measures.

Figure 1. Three main models of data ownership in healthcare

2.1 Private ownership

In this model, patients or individuals retain full ownership of their healthcare data. They have the right to control, share or sell their data as they see fit. Advocates argue that this approach empowers individuals and promotes their autonomy by giving them control over their personal health information. However, critics point out that this approach may not incentivize efficient use of the data for broader societal benefits, such as public health research, especially when access to the data is restricted behind paywalls or otherwise [19].

2.2 Public ownership

Healthcare institutions, governments or public entities hold ownership of healthcare data. This model enables the aggregation of data for research, policy development and public health initiatives. Supporters argue that public ownership fosters transparency, equitable access and ensures that the data is used for the common good. However, it can also raise concerns over privacy, security and the risk of misuse, particularly when patients have limited control over who accesses their information [19].

2.3 Hybrid ownership

This model strikes a balance by allowing patients to own their data while granting [8] healthcare institutions and researchers specific usage rights. This approach often requires patient consent for access or use, aligning with principles of autonomy and control. The hybrid model is seen as a potential solution to the challenges posed by both the private and public ownership models, but requires a robust infrastructure for tracking consent and protecting data privacy. Many countries are developing frameworks that permit shared data ownership so that patients retain control over their data, while granting healthcare providers and researchers access for legitimate purposes. This approach aims to balance the needs of data privacy with the advantages of data sharing for public health and medical research. The differences between these 3 main models of data ownership in healthcare are shown in Table 1.

2.4 Practical applications and real-world examples

In practice, the application of these models varies. For instance, patient registries often involve complex ownership structures, especially if the data is sourced from multiple entities such as hospitals, clinics and research institutions. Clearly defining and legally documenting data ownership is crucial in these contexts to ensure ethical use and regulatory compliance.

2.4.1 Consent management frameworks for health information exchange

The proliferation of health information exchanges (HIEs) has transformed healthcare delivery and facilitated the seamless sharing of electronic health records (EHRs) across various providers and institutions [21]. However, safeguarding patient privacy and ensuring consent for data sharing are paramount. Developing robust consent management frameworks within HIEs is essential to respect patient autonomy and comply with privacy regulations [22]. These frameworks must take into account the varying degrees of consent that patients may wish to exercise regarding the sharing of their personal health information (PHI). The integration of advanced technologies such as blockchain, AI and machine learning (ML) can offer solutions to the complexity of dynamically managing patient consent while ensuring security and traceability [23]. Additionally, patient education and engagement are vital for the success of consent management frameworks, as they ensure that patients are fully informed about their rights and the consequences of giving or withholding consent.

Table 1. Comparisons between three models of data ownership [20, 21]

	Private Ownership	**Public Ownership**	**Hybrid Ownership**
Ownership	Patients or individuals retain full ownership of their healthcare data.	Healthcare institutions, governments or public entities hold ownership of healthcare data.	Patients retain ownership, but healthcare institutions and researchers are granted specific usage rights.
Control	Individuals can control, share or sell their health data as they see fit.	Patients have limited control over who accesses their data.	Requires patient consent for access, preserving individual control and autonomy.
Principles	Autonomy: Empowers individuals by giving them control over their data.	Common good: Data usage focuses on societal benefits, promoting transparency and equity.	Balance: Combines private and public models, balancing individual rights and societal benefits.
Privacy	Ensures privacy by allowing individuals to decide on data access.	Increase risk as patients have limited control, potentially affects data security.	Ensures privacy with controlled data sharing based on consent.
Utilization	Economic opportunity: Allows individuals to monetize their data.	Aggregation for research: Facilitates data aggregation for public health research and policy.	Research access: Enables controlled access for researchers while respecting patient rights.
Concerns	Challenges for public health: Data sharing may be limited, impacting public health research.	Misuse risk: Potential for data misuse if security measures are inadequate.	Infrastructure needs: Requires robust infrastructure to manage consent and data protection.
Access	Restricted access: Data access may be hindered by paywalls, limiting research and initiatives.	Access control: Institutions control access, often prioritize public health over individual control.	Flexible model: Seen as a balanced approach but can be complex to implement.
Sharing	Lack of Incentives: May not encourage data sharing for collective benefits.	Transparency: Promotes equitable access and data usage for societal benefits.	Flexible use: Enables data sharing for both individual and societal benefits through a consent model.

2.4.2 Blockchain-based consent models

Blockchain technology offers innovative solutions for consent management in healthcare. A study introduced a blockchain-based consent model of data sharing for controlling access to individual health data [24]. This model utilizes smart contracts to dynamically represent individual consent and enable data requesters to search and access data. The evaluation indicated that such a data sharing model provides a flexible approach to deciding how data is used by requesters, while ensuring that individual consent is respected and accountability is maintained [25].

2.4.3 Consentio: managing consent with permissioned blockchains

Another approach, Consentio, is a scalable consent management system based on the Hyperledger Fabric permissioned blockchain. It addresses the challenge of ensuring high throughput and low latency in endorsing data access requests and granting or revoking consent. Experimental results show that Consentio can handle as many as 6,000 access requests per second, which allows it to scale to very large implementations.

2.4.4 Hybrid data storage in healthcare

The approaches of hybrid data storage, combining on-premises infrastructure with cloud services, are becoming more popular in healthcare. This model offers flexibility to meet the needs of healthcare organizations, allowing patients' sensitive information to be securely stored on-site, while less critical data can be stored in the cloud to facilitate access and scalability [26]. The hybrid model addresses data challenges in healthcare by striking a balance between control and flexibility and enabling medical practices to respond quickly to changing data demands [27]. However, implementing a hybrid data storage system may be more complicated than traditional on-premise or pure cloud solutions and requires technical expertise and resources to ensure smooth operation across various settings.

The landscape of privacy regulations and consent frameworks in healthcare varies significantly across the globe, reflecting diverse legal, cultural and technological contexts. To understand the adoption and implementation of privacy models and consent frameworks is essential for navigating the complexities of patient data protection in different regions.

2.5 Global adoption of privacy models in healthcare

Privacy models in healthcare are designed to safeguard patient information and ensure compliance with legal standards. Three prominent models include:

The European Union's General Data Protection Regulation: Enforced in 2018, GDPR has set a global benchmark for data protection and influenced legislation in various countries, including Brazil, Japan and South Korea. Its principles emphasize data minimization, purpose limitation and explicit consent, making it a widely adopted framework in many jurisdictions [28].

The Health Insurance Portability and Accountability Act in the United States: HIPAA establishes national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers. It focuses on protecting patient health information from fraud and theft and ensures data privacy and security in the U.S. healthcare system [29].

The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada: PIPEDA regulates how private sector organizations collect, use and disclose personal information in the course of commercial activities, including healthcare services. It mandates that consent must be obtained for data collection and provides individuals with the right to access and correct their personal information [30].

These models are not universally adopted; their implementation depends on regional legal frameworks and cultural attitudes toward privacy. For instance, while GDPR's influence is expanding, countries such as the United States maintain distinct regulations, such as HIPAA, which are tailored to their specific legal and healthcare environments.

3. Ethical and legal frameworks for patient data

Ethical and legal frameworks [10] for handling patient data are essential for safeguarding privacy, ensuring transparency and maintaining trust. These frameworks consist of core components (Figure 2) that collectively guide the responsible management of patient information. Understanding how these components have been defined, their global acceptance and their adoption in healthcare regulations is crucial for comprehending their current application.

3.1 Confidentiality

Confidentiality mandates that patient information remains accessible only to authorized individuals to prevent unauthorized access or disclosure [21]. This principle is enshrined in various international regulations, such as the HIPAA in the United States and the GDPR in the European Union. These regulations set standards for electronic health transactions and protect the privacy of health information by emphasizing the need for consent, data minimization and the right to access personal information.

3.2 Informed consent

Consent is crucial, especially for secondary uses such as research, where patients' autonomy in decision-making must be respected. Informed consent requires that patients are fully aware of and agree to the collection, use and sharing of their data [31]. This concept is a cornerstone of ethical medical practice and is embedded in healthcare regulations worldwide. For instance, the GDPR mandates that personal data, including health information, must be processed lawfully, fairly and transparently, with the consent of the data subject.

3.3 Ownership and data rights

There is an ongoing debate about data ownership. Some frameworks support the notion that patients should "own" their data and control access, particularly in cases where data may be shared with third parties for commercial purposes [10, 21]. This issue is complex and varies across jurisdictions. For example, the GDPR grants individuals the right to access and control their personal data, including health information.

3.4 Security measures

Security measures are essential to protect patient data from unauthorized access and breaches. Regulations such as HIPAA and GDPR mandate strict data protection standards, including encryption, access controls and breach notification policies. These measures are designed to safeguard patient data and maintain trust in healthcare systems [22].

3.5 Ethical use of data in emerging technologies

As healthcare integrates technologies such as AI and the Internet of Things (IoT), ethical frameworks emphasize fairness, transparency and regulatory compliance. These frameworks ensure that data-driven decisions respect patient rights and do not lead to discriminatory practices. For instance, the GDPR includes provisions on automated decision-making, including profiling, to protect individuals from potential harms [23].

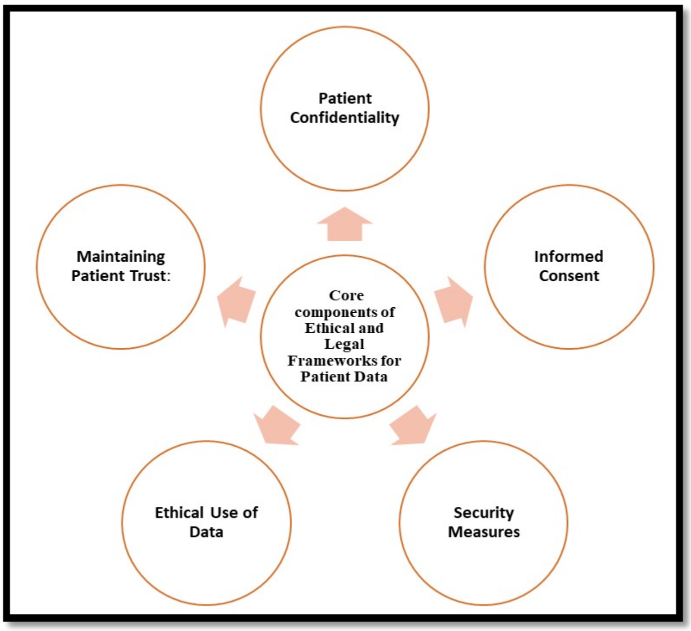
Patient Confidentiality
Maintaining Patient Trust:
Informed Consent
Core components of Ethical and Legal Frameworks for Patient Data
Ethical Use of Data
Security Measures

Figure 2. Ethical and legal frameworks components for patient data

3.6 Maintaining patient trust

Maintaining patient trust is vital for effective delivery of healthcare. Ethical guidelines emphasize the importance of transparency to enable patients to feel secure about sharing their data for personal care and potential health advancements. Trust is built through clear communication about data usage and robust data protection measures [6].

4. Models of data privacy and consent

4.1 Traditional consent

Traditional consent models are relatively simple and require patients to give broad, one-time consent for the use of their healthcare data at the time of treatment. This consent typically lacks the flexibility to adjust or withdraw permissions once granted [6]. It relates primarily to data usage in the clinical settings, with little regard for changes in how data may be used over time. Although this model has been widely used in healthcare, it fails to capture the complexities of modern healthcare data usage, where data is shared across diverse contexts such as research, clinical trials and commercial purposes.

4.2 Emerging consent models

In contrast to the traditional model, emerging consent models focus on providing patients with greater control over their data. Digital and dynamic consent systems are central to this shift. These systems empower patients to specify, monitor and update their consent preferences over time to ensure that consent remains relevant to the evolving uses of their data [24]. These models aim to improve patient autonomy and provide transparency and flexibility. For example, patients can grant permission for their data to be used in specific research studies and to be only shared with designated providers or organizations. Furthermore, these systems support the ability to revoke consent or modify it as necessary, which strengthens patient engagement and trust [25]. Granular consent allows patients to provide detailed and specific authorizations for the use of their health data [26]. This model enables patients to give consent for particular uses, such as sharing data with certain healthcare providers, participating in research studies or storing data in specific databases. It is a more nuanced approach compared to traditional consent, which tends to be broad and less adaptable. Granular consent models enhance transparency by offering patients clear choices about how and with whom their data is shared, fostering a stronger sense of control and involvement. This model aligns with the growing demand for tailored, patient-centric care, where data usage is transparent and under the control of patients [28]. Figure 3 illustrates a comparison of data privacy and consent models, highlighting the distinctions among traditional, emerging and granular consent approaches in terms of flexibility, transparency and patient control.

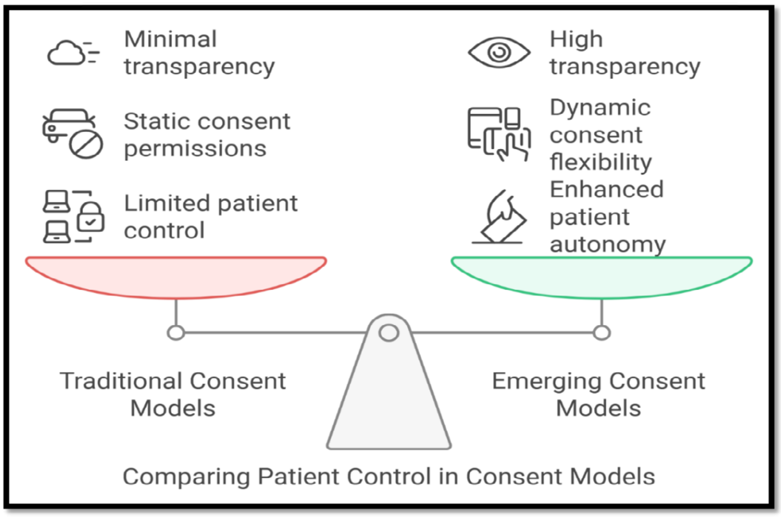
Minimal transparency
Static consent permissions
Limited patient control
High transparency
Dynamic consent flexibility
Enhanced patient autonomy
Traditional Consent Models
Emerging Consent Models
Comparing Patient Control in Consent Models

Figure 3. Comparison of data privacy and consent models

4.3 Patient preferences and data use

When designing consent frameworks, it is critical to consider patients' preferences, ensuring that their data is used in ways that align with their personal values and concerns. Different consent models, such as "opt-in" and "opt-out", define how data can be shared [29]. In an "opt-in" framework, patients actively choose to share their data for specific purposes, while in an "opt-out" model, patients are automatically included unless they decline to participate [30]. These approaches need to be flexible enough to accommodate ongoing changes in patient preferences and concerns. Platforms that take these preferences into account should offer easy-to-use mechanisms for patients to modify their consent, helping them retain control over their personal health data as it moves through different healthcare systems. Ultimately, the evolution from traditional to emerging consent models marks a significant shift towards greater transparency, control and respect for patient autonomy, allowing patients to determine how their health data is used throughout their care journey [32].

5. Patient-centred data consent frameworks

Patient-centered data consent frameworks are essential for enhancing patient autonomy and control over personal health information in healthcare [33]. The frameworks of patient-centered consent should be based on the patient's goals and priorities [34]. They are built on several key principles aimed at empowering patients while ensuring transparency and privacy. These frameworks aim to empower patients by allowing them to actively participate in decisions about how their health data is collected, shared and used. This approach aligns with evolving privacy models, regulations and technological advancements that prioritize transparency, choice and trust in data handling within the healthcare system.

5.1 Types of patient-centred consent models

The various consent models such as dynamic, tiered, one-time with periodic renewal, event-triggered and opt-out with notifications (Figure 4) offer flexible approaches to informed consent, allowing patients to control, modify and stay informed about the use of their health data in different research and healthcare settings.

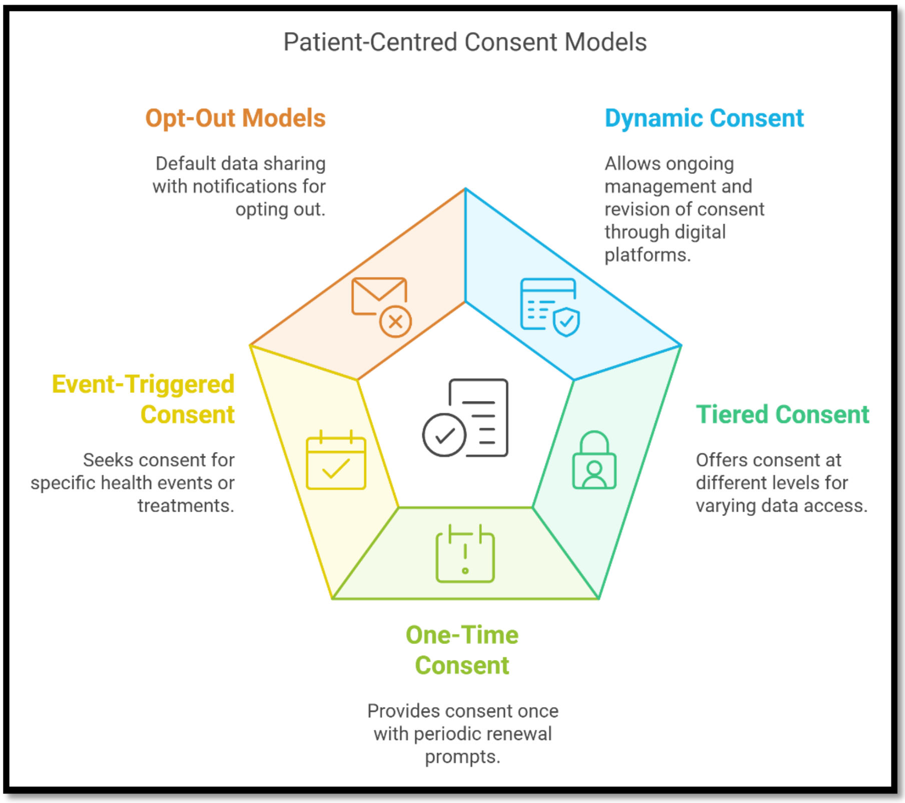
Patient-Centred Consent Models
Opt-Out Models
Default data sharing with notifications for opting out.
Dynamic Consent
Allows ongoing management and revision of consent through digital platforms.
Event-Triggered Consent
Seeks consent for specific health events or treatments.
Tiered Consent
Offers consent at different levels for varying data access.
One-Time Consent
Provides consent once with periodic renewal prompts.

Figure 4. Types of Patient-centered Consent models

5.1.1 Dynamic consent

The dynamic consent model is used for informed consent that emphasizes ongoing, interactive engagement with participants [35]. In contrast to static models, dynamic consent allows participants to make granular, real-time decisions about the use of their data or biological samples [36]. This is facilitated through digital platforms where individuals can provide, modify or withdraw consent at any point. This model is particularly relevant in longitudinal studies and biobanking, ensuring transparency and fostering trust [37]. Additionally, dynamic consent supports personalized communication, enhancing participant understanding and autonomy while addressing ethical concerns related to data sharing and reuse in modern research settings.

5.1.2 Tiered or layered consent

Tiered or layered consent is a patient-centered model that provides flexibility and autonomy by allowing participants to choose consent levels for various aspects of a study. The tiered approach offers specific options, such as participation in only certain types of research or data-sharing agreements, while the layered model simplifies the presentation of information by providing essential details upfront and offering more detailed content for those interested. This model is particularly effective in genomic and biomedical research, fostering patient trust and engagement by tailoring the consent process to individual preferences [38].

5.1.3 One-time consent with periodic renewal

One-time consent with periodic renewal is a model that balances simplicity with adaptability. In this approach, participants provide a single, comprehensive consent at the start, which remains valid but is reviewed periodically for updates or reaffirmation. This model ensures that patients remain informed of changes in study scope, risks or benefits over time, fostering trust and transparency. It is especially suitable for a long-term research, such as learning health systems and genomic studies, where ongoing engagement and data use evolved.

5.1.4 Event-triggered consent

Consent is sought for specific health events, such as a new diagnosis, treatment plan or the start of a new healthcare relationship. This model ensures that patients only consent to the sharing of data relevant to specific care events. For example, a patient newly diagnosed with diabetes may be asked for consent specifically for data sharing for diabetes research or new treatments. If the same patient later starts a novel treatment for heart disease, consent will be requested again, specifically for sharing of heart-related data. In this way, the patient only consents to the use of data relevant to specific diagnoses and treatments as their healthcare needs evolve [39].

Table 2. Benefits of patient-centered consent frameworks

Consent Model	Dynamic Consent	Tiered or Layered Consent	One-Time Consent with Periodic Renewal	Event-Triggered Consent	Opt-Out Models with Notifications
Ownership	Participants retain ownership and actively manage their data.	Participants retain flexible ownership based on consent level chosen.	Ownership remains with participants but will be periodically reaffirmed.	Ownership is tied to specific healthcare events or diagnoses.	Default ownership rests with institutions; participants can withdraw consent.
Control	Full control to modify, provide or withdraw consent at any time via digital platforms.	Control is tailored to chosen levels of involvement in research.	Control maintained through periodic reaffirmation of consent.	Consent and control are specific to particular health events.	Notifications provide ongoing control to withdraw consent for specific exchanges.
Principles	Promotes autonomy, transparency and participant-researcher collaboration.	Supports autonomy and flexibility while simplifying decision-making.	Balances simplicity with adaptability and ongoing engagement.	Ensures relevance and ethical practice by focusing on specific scenarios.	Balances efficiency in data sharing with individual autonomy and transparency.
Privacy	High: Participants decide who accesses their data and when.	High: Privacy ensured through granular and tailored consent options.	Moderate: Privacy is maintained through regular consent updates.	High: Limits data sharing to specific, relevant healthcare events.	Moderate: Participants are informed of data usage but default sharing may pose risks.
Utilization	Ideal for longitudinal studies, biobanking, and personalized research.	Effective for genomic and biomedical research requiring participant trust.	Suitable for long-term studies with evolving research needs.	Enables targeted research tied to specific health events and diagnoses.	Facilitates broad data usage for public health and research while retaining control.
Concerns	Complex implementation requiring digital infrastructure and ongoing engagement.	May limit large-scale aggregation if participants opt for a lower involvement.	Re-engagement may be burdensome for participants and researchers.	Challenging to manage consent for multiple and evolving health events.	Risk of disengagement due to notification fatigue or lack of active participation.
Sharing	Encourages collaboration with consent-based and transparent sharing.	Tailored to individual preferences while promoting trust in sharing.	Ensures ethically sound sharing adapted to study progress.	Data shared selectively, focusing on relevance to the participants' context.	Enables broad sharing while maintaining the ability to withdraw consent easily.

5.1.5 Opt-out models with notifications

Some frameworks may use opt-out consent, where data sharing is the default setting, but patients are notified each time data is shared. They can then decide to restrict access if they want to retain the control over their information. For example, in a regional health information exchange (HIE), patient data is shared by default to improve care coordination. Each time their data is shared across facilities or with new providers, patients receive a notification (via email or SMS) and can opt out if they wish. This approach keeps patients informed about the sharing of their health data while allowing them to easily withdraw consent for specific exchanges, giving them flexibility and ongoing control.

5.2 Benefits of patient-centered consent frameworks

Table 2 provides a comparative overview of various consent models, highlighting the unique benefits each framework offers in facilitating ethical, transparent and participant-centered approaches to data sharing and research participation.

6. Understanding privacy models and consent frameworks

Privacy models are structured approaches that dictate how personal data is collected, processed and shared. Consent frameworks, on the other hand, establish guidelines for obtaining and managing users' consent regarding their data. Together, they aim to ensure that organizations handle personal information responsibly and transparently.

6.1 Risks associated with privacy models and consent frameworks

6.1.1 Inadequate risk management

A lack of a well-defined privacy risk management framework can result in ineffective data validation and protection. Without a structured approach:

- Organizations may fail to identify vulnerabilities, leading to data breaches.
- Compliance risks increase, as businesses might unknowingly violate data protection regulations.
- Data governance inefficiencies may arise, making it difficult to enforce policies consistently.
- Consumers' trust erodes if their data is mishandled, which potentially leads to reputational damage.

Example: A healthcare provider who does not integrate risk management into its privacy framework may fail to detect unauthorized access to medical records, leading to regulatory penalties and loss of consumer trust.

6.1.2 Lack of standardization

The absence of standardized privacy and security protocols across industries results in inconsistent data protection. This increases susceptibility to cyber threats in multiple ways:

- Non-standardized security practices lead to interoperability issues, resulting in system vulnerabilities.
- Inconsistent data protection measures across global jurisdictions complicate compliance efforts.
- Organizations may struggle to enforce uniform policies for third-party vendors, increasing the risk of data leaks.

Example: A multinational e-commerce platform operating under different regulatory frameworks may fail to align its security protocols, leading to gaps that cybercriminals can exploit.

6.1.3 Insufficient legal frameworks

A weak legal foundation makes it difficult to enforce privacy rights, leading to:

- Unclear regulations that leave service providers unsure of their data protection obligations.
- Inadequate penalties, which fail to deter malicious actors from exploiting weak systems.
- Ambiguities in the user consent and data usage policies, allowing for potential misuse of personal data.

Example: A country without strict data protection laws may allow companies to collect biometric data without user consent, increasing the risk of unauthorized surveillance.

6.1.4 Emerging technologies

New technologies such as AI, machine learning and blockchain bring unique challenges for data protection:

- AI-driven profiling can lead to biases, discrimination and privacy intrusions.
- Automated data processing can make it difficult to track how personal data is used.
- Lack of AI governance frameworks may lead to unintentional privacy breaches.

Example: A facial recognition system used in public spaces may collect and store biometric data without clear consent, raising ethical and legal concerns about mass surveillance.

6.1.5 Inadequate threat modeling

Without systematic modeling of privacy threat, organizations fail to anticipate and mitigate potential risks.

This results in:

- Increased exposure to insider threats and malicious actors.
- Unidentified vulnerabilities that may be exploited in cyber-attacks.
- Reactive instead of proactive privacy protection strategies.

Example: A financial services firm that does not conduct privacy threat modeling may overlook vulnerabilities in its online banking system, leading to unauthorized data access by hackers [34].

6.2 Recent developments and emerging risks

Recent privacy reforms, such as those in Australia, require companies to response immediately to avoid legal repercussions. These changes, highlighted by a new "privacy tort," require companies to align with stricter data practices within six months or face potential legal action due to harmful or invasive data practices. Additionally, the role of Chief Privacy Officers (CPOs) is expanding to include responsibilities in the areas of artificial intelligence and cybersecurity. Privacy executives are now ensuring compliance with evolving data protection laws and are involved earlier in product development to address privacy concerns from the design phase.

To address these risks, organizations should consider the following strategies:

- Implement robust management on privacy risk: Designing a privacy risk management framework is critical to ensure the validation and protection of data and compliance with all applicable laws and regulations.
- Adopt standardized protocols: Implementing standardized protocols can enhance data protection measures and reduce vulnerability to cyber threats.
- Establish comprehensive legal frameworks: Developing legal structures that safeguard individual data, privacy and user rights is essential to protect data from breaches.
- Address emerging technology risks: Identifying and addressing privacy concerns related to emerging technologies, such as artificial intelligence, is vital to ensure data security.
- Conduct privacy threat modeling: Systematically identifying and addressing potential privacy issues in systems and applications can help mitigate vulnerabilities.
- By implementing these strategies, organizations can safeguard user data, maintain compliance and build consumer trust in an evolving digital landscape.

6.3 Implementation of consent frameworks in healthcare

Consent frameworks are critical for ensuring that patients have control over their personal health information. The adoption and implementation of these frameworks varies across regions and is influenced by local regulations, technological infrastructure and cultural attitudes toward privacy.

Europe: General data protection regulation

In Europe, the GDPR serves as a cornerstone for data protection, including in the healthcare sector. The GDPR mandates that healthcare organizations must obtain explicit and informed consent from individuals before processing their personal data. This regulation emphasizes transparency, accountability and the protection of personal data and ensures that individuals have control over their health information [35].

Asia-Pacific: Diverse approaches to consent

The Asia-Pacific region exhibits a diverse landscape regarding consent frameworks in healthcare:

Singapore: The Personal Data Protection Act (PDPA) requires organizations to appoint a Data Protection Officer (DPO) and make their business contact information publicly accessible. While consent is a legal basis for processing personal data, the PDPA allows for processing without consent in certain situations, such as for the "vital interests of individuals" or "matters affecting the public" [36].

China: Regulators have sought to restrain "bundled consent" in baseline texts such as the Personal Information Security Specification and the Personal Information Protection Law, aiming to ensure that consent is specific and informed.

India: In August 2023, India enacted the Digital Personal Data Protection Act of 2023 (DPDP), which defines "Personal Data" broadly and applies to the processing of digital personal data both inside and outside India. The DPDP imposes various consent, notice and public reporting obligations on digital health providers operating in India [37].

United States: health insurance portability and accountability act

In the United States, the HIPAA requires covered entities to obtain patient consent before using or disclosing protected health information for treatment, payment or healthcare operations, with certain exceptions. HIPAA aims to protect patient privacy and ensure the confidentiality of health information [38] .

6.4 Enhancing patient data privacy and security: addressing the limitations of GDPR and HIPAA

6.4.1 General data protection regulation (GDPR) in Europe

In Europe, the General Data Protection Regulation (GDPR) stands as a cornerstone for the protection of patient data privacy. It mandates that healthcare organizations must obtain explicit consent before processing personal data. The regulation emphasizes transparency, accountability and ensuring that individuals have control over their health information [39]. However, there are challenges in managing consent in emergency situations where obtaining explicit consent may not be feasible, and when data is repurposed for research or AI models, which may conflict with the GDPR's principle of data minimization. Additionally, the GDPR's strict rules on cross-border data transfers complicate the collaboration with international partners, such as pharmaceutical companies and tech firms.

Blockchain technology can address these issues by providing a decentralized, transparent system for tracking patient consent, allowing individuals to manage who accesses their data and revoke consent when necessary. Furthermore, AI techniques such as federated learning and differential privacy can ensure that patient data is not centralized and that sensitive information remains private during analysis and training, in line with GDPR's requirements for data minimization.

6.4.2 Health insurance portability and accountability act (HIPAA) in the United States

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) is critical to protecting patient health information (PHI), as it by requires covered entities to obtain patient consent before using or disclosing PHI for treatment, payment or healthcare operations. Despite its critical role in safeguarding privacy, HIPAA also has its limitations. For example, it only applies to specific healthcare providers and entities, leaving gaps when third-party vendors or technology companies access PHI. Additionally, HIPAA also lacks a fully flexible system for managing consent preferences, as patients may not be able to specify what types of PHI they are would like to share [40].

Blockchain can help bridge these gaps by providing a secure, immutable platform that tracks patient consent in a granular way, ensuring transparent access to PHI and improving accountability. AI can further support HIPAA compliance by offering advanced encryption techniques and anomaly detection in data access patterns, reducing the risk of breaches and maintaining the confidentiality of patient information.

6.4.3 The role of emerging technologies in overcoming regulatory limitations

Both GDPR and HIPAA have shaped the landscape of patient data protection, but emerging technologies such as blockchain and AI offer innovative solutions to overcome their limitations. Blockchain's decentralized structure can ensure that patient consent is managed transparently and securely, addressing concerns about data access and control [41]. AI, particularly through privacy-preserving techniques such as federated learning and differential privacy, can help ensure that sensitive health data remains protected during the analysis process without compromising regulatory compliance [31]. These technologies provide a path forward to create more secure, adaptable systems that empower patients, ensure privacy and align with evolving regulations.

7. Emerging technologies and patient privacy

The integration of emerging technologies such as blockchain and AI [42] into healthcare is revolutionizing patient privacy and autonomy, offering new ways to safeguard sensitive data while empowering patients with control over their health information [43]. An overview of how these technologies contribute to enhancing patient privacy and data ownership through innovative privacy models and consent frameworks is presented as follows.

7.1 Blockchain technology

Blockchain technology in healthcare provides a decentralized ledger system that stores encrypted patient data across multiple nodes, ensuring that the data cannot be accessed or altered without detection [44]. This decentralization and immutability ensure that patient records are secure, as they are distributed across the network rather than stored in a centralized database [45, 46]. Blockchain reduces the risk of unauthorized access and fosters transparency [47], as any attempt to alter data requires consensus from the network, making tampering easy to detect [48]. Furthermore, it also empowers patients to control their data by granting and revoking access to their medical records without relying on intermediaries, such as insurance companies or centralized repositories. For example, MedRec [49], a blockchain-based system, allows patients to manage access to their records while enabling secure and transparent data sharing among healthcare providers with their consent. The benefits include improved data security, increased transparency in data management and greater patient control over personal health information [50].

7.2 Artificial intelligence technology

Artificial Intelligence (AI) has the potential to transform healthcare by improving diagnostics, personalizing treatment plans and enhancing care quality [51]. However, the use of AI often requires access to large datasets containing sensitive patient data, which raises privacy concerns. To address these concerns, privacy-preserving AI techniques such as federated learning and differential privacy are being developed. Federated learning allows AI models to be trained on decentralized data sources, such as local healthcare facilities or patient devices, without transferring raw data to a central server [31]. This ensures that sensitive data remains private while still enabling AI models to learn from a broad dataset. In contrast, differential privacy adds noise to data to protect individual privacy while still allowing for meaningful analysis at a population level. These techniques enable the development of AI models that improve healthcare outcomes without compromising patient privacy. They protect patient information, reduce the need for centralized data storage and ensure that sensitive data is not exposed during the AI training process. Thus they offer a secure approach to utilizing AI in healthcare [52].

7.3 Blockchain and AI for enhanced privacy and autonomy

When blockchain and AI are combined, healthcare systems can achieve higher levels of privacy and security for patient data. Blockchain ensures that the data is securely encrypted and decentralized, while AI can analyze the data without compromising patient privacy through methods such as federated learning and differential privacy [53].

In a combined blockchain and AI system, a patient's health data could be securely stored on a blockchain, with access granted only to authorize healthcare providers. The AI system, utilizing federated learning, would analyze this data across multiple healthcare institutions without transferring the sensitive data itself. This ensures that patient data remains private but can still be used to inform critical healthcare decisions. The benefits of such a system include a higher level of security and privacy due to the synergy between the decentralization of blockchain and privacy-preserving techniques through AI. It also provides greater patient autonomy, allowing patients to control both access to and the use of their data, while benefiting from AI-driven insights. Additionally, it enhances trust in healthcare systems, as patients are reassured that their sensitive data is protected, even as it contributes to improving healthcare outcomes [54].

Emerging technologies such as blockchain and AI are transforming privacy models in healthcare, enabling more secure and patient-centric approaches to data management. Blockchain offers enhanced security, decentralization and patient control [44], while AI techniques such as federated learning and differential privacy help ensure that data can be analyzed without compromising privacy [55]. Together, these technologies provide a powerful framework to ensure patient autonomy in data ownership, foster trust in healthcare systems and safeguard sensitive health information [56]. The integration of AI and blockchain in healthcare faces challenges such as data breaches, algorithmic bias and inconsistent privacy laws. Blockchain ensures secure, decentralized data management with smart contracts automating consent processes, while federated learning enables data analysis without exposing sensitive information. Addressing AI bias requires transparent model development and regular audits, while harmonized global privacy standards can eliminate legal inconsistencies. To empower patients, adaptive consent interfaces and education initiatives are essential. Advancing encryption, real-time monitoring and interoperable systems will foster a healthcare ecosystem that prioritizes innovation, privacy and patient autonomy.
Several significant studies highlight the potential of AI in securing sensitive medical data while ensuring effective utilization for diagnosis, treatment and research.

7.3.1 Privacy-enhanced strategies in healthcare 4.0

The study "A Privacy-Enhanced Multiarea Task Allocation Strategy for Healthcare 4.0" introduced innovative strategies to protect the privacy of medical data while ensuring that healthcare systems can still efficiently allocate tasks and resources across multiple areas [57]. This research discussed the importance of privacy preservation in Healthcare 4.0, which involves the integration of AI, IoT and other advanced technologies into healthcare settings. By using privacy-enhanced task allocation methods, this strategy enables healthcare systems to leverage AI without compromising patient privacy, ensuring data flow securely across multiple sectors [58].

7.3.2 Federated learning in disease diagnosis

Another pivotal work, "Federated Learning-Empowered Disease Diagnosis Mechanism in the Internet of Medical Things: From the Privacy-Preservation Perspective," explored the integration of federated learning in the Internet of Medical Things (IoMT) [59]. Federated learning allows AI models to be trained on distributed data sources (e.g., data from multiple hospitals or medical devices) without transferring patients' sensitive data to a central server, thus can significantly enhance the level of privacy protection. This study highlighted how federated learning can be applied in disease diagnosis and enable AI systems to make accurate predictions while preserving patient confidentiality. It is a promising approach for developing healthcare systems that prioritize both data privacy and diagnostic accuracy.

7.3.3 Hierarchical federated learning for anomaly detection

The study "Toward Accurate Anomaly Detection in Industrial Internet of Things Using Hierarchical Federated Learning" introduced a hierarchical federated learning, a technique that can improve the accuracy of anomaly detection while safeguarding privacy [27]. While this study primarily focused on industrial applications and the methodology is highly applicable to healthcare, particularly in detecting anomalies within large healthcare datasets. By training models in a hierarchical and decentralized manner, AI can detect unusual patterns or security breaches in medical data while maintaining the privacy of patients' individual information. This can be particularly important in healthcare, where detecting data breaches or security threats is critical to safeguarding patient privacy.

7.3.4 AI's impact on privacy in medical data

These works collectively underscore AI's potential to enhance privacy in healthcare. Through techniques such as federated learning, hierarchical federated learning and privacy-enhanced task assignment, AI can provide effective and secure solutions for processing and analyzing sensitive medical data. These methods allow healthcare providers to gain valuable insights from patient data without compromising privacy, representing a significant improvement over traditional centralized data storage models. Additionally, these privacy-preserving AI techniques are in line with regulatory frameworks such as GDPR and HIPAA, ensuring compliance while still enabling innovation in medical diagnostics and treatment. Incorporating these key studies will enrich the discussion on the role of AI in medical data privacy and illustrate how emerging technologies are shaping the future of secure, privacy-conscious healthcare systems.

7.4 Limitations

Blockchain and AI offer transformative potential for healthcare data management, yet they also have notable limitations that must be addressed to ensure effective and secure implementation.

7.4.1 Limitations of blockchain in healthcare data management

Scalability and performance issues: Blockchain networks, particularly public ones, often face scalability challenges due to low transaction throughput and latency [61]. As the volume of healthcare data grows, these limitations can lead to network congestion and slower processing times, hindering real-time data access.

Integration into existing systems: Incorporating blockchain with current healthcare infrastructures is complex. Compatibility issues and data migration challenges can impede seamless integration and require significant coordination among diverse healthcare systems.

Challenges in Data standardization: Healthcare data is often fragmented and stored in different formats, making standardization difficult [41]. This lack of uniformity hinders interoperability and data sharing across blockchain platforms and limits their effectiveness.

Regulatory and legal concerns: Navigating the complex landscape of healthcare regulations, such as HIPAA and GDPR, poses significant challenges to blockchain adoption [61]. Ensuring compliance across different jurisdictions requires a careful consideration and alignment with legal standards.

Security and privacy risks: Even though blockchain offers inherent security features, it is not immune to vulnerabilities. Potential risks include errors in smart contracts and data breaches, which require robust security measures to protect sensitive patient information [63].

7.4.2 Limitations of AI in healthcare data management

Data privacy and security concerns: AI systems require extensive patient data, raising concerns about data breaches and privacy violations [63]. Implementing stringent data protection measures is essential to mitigate these risks.

Bias and fairness issues: AI algorithms trained on historical data may perpetuate existing biases, leading to disparities in treatment recommendations or diagnoses [64]. Ensuring diverse and representative datasets is crucial to overcome this challenge.

Lack of interpretability and explainability: Many AI models operate as "black boxes", making it difficult for healthcare professionals to understand the rationale behind AI-generated decisions [65]. This opacity can hinder trust and acceptance of AI tools in clinical settings.

Integration into existing healthcare systems: Introducing AI into current healthcare infrastructures can be complex, especially when legacy systems are involved. In order to achieve seamless integration, interoperability standards and investing in IT infrastructure are required.

Legal and ethical considerations: The use of AI in healthcare raises legal and ethical issues, particularly regarding accountability for AI-driven medical decisions [66]. A balance between human oversight and AI autonomy is essential to maintain patient safety and ethical standards.

7.4.3 Limitations of privacy-preserving AI techniques

While federated learning and differential privacy are recognized as important methods for preserving privacy in AI applications, especially in sensitive fields such as healthcare, both techniques have inherent limitations in their ability to fully protect data. These limitations are widely discussed in the literature and highlight the challenges that arise in achieving both privacy and utility. The specific weaknesses of these two approaches are examined in detail below.

Federated learning: privacy risks and vulnerabilities

Federated learning is a decentralized approach to machine learning where the data is stored locally on the devices and only model updates are shared with the central server. This helps prevent raw data from leaving the device, thereby enhancing privacy. However, federated learning is still vulnerable to several significant privacy risks.

Model inversion attacks: One of the major concerns with federated learning is the potential for model inversion attacks. In this scenario, attackers can analyze the updates shared between the devices and the central server to reverse engineer and reconstruct sensitive data that was used to train the model [67]. Despite the decentralized nature of federated learning, attackers can still extract private information, making this a critical vulnerability.

Data leakage through model updates: Even though raw data is not transferred, the model updates (i.e., gradients or weights) sent to the server can unintentionally leak private information. If an attacker has access to these updates, they may be able to infer patterns in the data, thereby exposing sensitive details.

Model poisoning: Another risk is model poisoning, where malicious participants inject corrupt data or model updates into the federated learning system. These poisoned updates can degrade the accuracy of the model or, in some cases, expose private information [68]. This is particularly problematic in scenarios where federated learning is used in healthcare, as the integrity of the model directly impacts decision-making and patient care.

Device security: Federated learning assumes that the devices involved in the training process are secure. However, if a device is compromised (for instance, by malware), private information could be leaked or model updates could be corrupted. This reliance on device security poses a significant challenge to maintaining privacy in a federated network [69].

Differential privacy: the challenges of balancing privacy and utility

Differential privacy adds a layer of noise to data or model outputs to obfuscate individual data points and protect privacy [70]. Although it has proven effective in many applications, particularly for large datasets, it also has significant limitations when it comes to simultaneously preserving privacy and utility.

Trade-off between privacy and utility: A key limitation of differential privacy is the trade-off between privacy and data utility. The more noise is added to the data to preserve privacy, the lower the accuracy and usefulness of the results will be [71]. In fields such as healthcare, where high accuracy is critical for diagnosis and treatment, this trade-off can undermine the effectiveness of AI models. Adding too much noise can result in a model that is too imprecise to offer actionable insights.

Membership inference attacks: Even though differential privacy is designed to protect individual privacy, it is not immune to membership inference attacks. These attacks enable an attacker to determine whether a specific individual's data is included in a dataset, even with noise added [72]. In healthcare, such attacks could compromise patient confidentiality, despite the use of differential privacy.

Reconstruction attacks: Another vulnerability of differential privacy is reconstruction attacks. In this type of attack, an attacker uses the noise patterns in the data to attempt to reconstruct the original data points [73]. Even when noise is applied, if the method is not carefully implemented, attackers could reverse engineer private information, which is a serious problem in medical data protection.

Privacy budget and parameter selection: Differential privacy requires the selection of a privacy budget that determines how much information can be released without violating privacy guarantees [74]. Finding the right balance in setting this budget is challenging—if it is set too high, privacy is compromised, and if it is set too low, the utility of the data is significantly reduced. This delicate balance is crucial, particularly in healthcare, where precision is essential for making medical decisions.

7.5 Adoption of AI privacy techniques and blockchain in the real world: healthcare applications

Both AI privacy techniques and blockchain technology have shown significant potential in transforming the healthcare sector, particularly in enhancing data privacy and security. While these technologies are still in the process of widespread adoption, there are notable real-world examples of healthcare systems and platforms that leverage these innovations to improve patient data security and streamline healthcare processes. Below, we examined some of the key real-world applications of AI privacy techniques and blockchain in healthcare.

7.5.1 AI privacy techniques in healthcare: real-world applications

AI privacy techniques, such as federated learning and differential privacy, are increasingly being utilized in healthcare systems to ensure the protection of sensitive medical data while still enabling valuable data-driven insights [34]. These techniques have been applied in several healthcare settings, focusing on privacy-preserving models for data analysis, disease prediction and personalized treatments.

Federated learning in healthcare: Federated learning is gaining traction in healthcare as it enables machine learning models to be trained across decentralized datasets, without sharing sensitive patient data. Some healthcare organizations have adopted federated learning to enhance medical research and clinical decision-making while preserving patient privacy.

Example: Google's federated learning for Health Google has worked on the projects involving federated learning for healthcare [75], such as using federated learning in partnership with the Mayo Clinic to improve medical imaging models. By training AI models locally on hospitals' data, this collaboration avoids the need for raw patient data to be shared across institutions, thereby safeguarding privacy while enabling improved diagnostic capabilities. Federated learning is also being used to analyze data from various wearable devices for the detection of early disease and personalized health recommendations without compromising patient confidentiality [76].

Differential privacy in healthcare: Differential privacy techniques are used to protect patients' individual data by adding noise to the data in such a way that the information cannot be traced back to a specific individual [77]. This method is particularly important when analyzing large datasets or sharing medical data for research purposes.

Example: Apple's health data privacy. Apple uses differential privacy to protect user data within its Health app [78]. By anonymizing and adding noise to aggregated health data, Apple enables researchers to perform useful health analytics without revealing individual data. This approach is particularly important for large-scale health studies, where it is critical to protect users' privacy while still gaining meaningful insights.

7.5.2 Blockchain technology in healthcare: real-world deployments

Blockchain has gained significant interest in healthcare for its ability to ensure data integrity, transparency and security. By providing a decentralized ledger, blockchain enables secure sharing of patient data across multiple stakeholders, reducing the risk of data breaches and ensuring that records cannot be altered without consensus. Some real-world examples of blockchain-based applications in healthcare are given below.

Blockchain for electronic health records (EHRs): Blockchain can revolutionize the management and sharing of electronic health records. By using a decentralized blockchain system, patients can have control over their health records, granting or revoking access to their data as needed while ensuring that records are tamper-proof and auditable [79].

Example: MedRec by MIT. Media Lab MedRec is a blockchain-based system developed by MIT Media Lab that allows patients to maintain control over their medical records. With MedRec, healthcare providers can access a patient's medical history in real-time while ensuring that the data is secure and immutable [80]. This decentralized approach eliminates the need for centralized databases, reducing the risks of data breaches. Patients can give consent for data sharing with providers, which improves transparency and data control.

Blockchain for supply chain management: Blockchain can also enhance the transparency and traceability of medical supplies and pharmaceuticals, ensuring that these products are authentic, properly handled and compliant with regulatory standards.

Example: FarmaTrust. FarmaTrust is a blockchain-based platform designed to improve the pharmaceutical supply chain by providing real-time tracking of drugs from manufacturers to consumers [81]. By using blockchain, FarmaTrust ensures the authenticity and safety of medicines, protecting consumers from counterfeit products. The platform's transparency ensures that stakeholders have access to trustworthy information about the origins and distributions of medical supplies.

Blockchain for medical research and clinical trials: Blockchain is being explored as a means to improve transparency and integrity in medical research, particularly in the management of clinical trials [82]. By creating a tamper-proof record of data collection and analysis, blockchain ensures the authenticity of research results, reducing the potential for fraud or data manipulation.

Example: ClinTex CTi. ClinTex CTi is a blockchain-powered platform that helps improve the efficiency and transparency of clinical trials [83]. It uses blockchain to create a secure and transparent record of clinical trial data, helping to reduce fraud and errors while ensuring that trial results are reliable. The platform also streamlines administrative processes, reducing the time and cost of bringing new drugs to market.

8. Case studies and practical applications

Implementing advanced models for data consent in healthcare systems is crucial for aligning with patients' expectations regarding privacy, control and transparency. Below are detailed case studies from different countries, highlighting their implementation processes, challenges encountered and outcomes achieved.

8.1 My Health Record (MHR) – Australia

Implementation process: Australia's My Health Record (MHR) is a nationwide digital health platform managed by the Australian Digital Health Agency. Initially launched as an opt-in system in 2012, it was transitioned to be an opt-out model in 2019 to increase participation [84]. MHR allows individuals to control access to their health data, enabling them to determine which healthcare providers can view or contribute to their records [84]. Privacy controls allow users to restrict access to specific information and set up alerts for unauthorized access attempts.

Challenges faced: The transition to an opt-out model raised significant concerns on privacy and security among the public [85]. A 2019 audit found that the system failed to adequately manage cybersecurity and privacy risks, with issues in ensuring legitimate emergency access and incomplete privacy assessments. Additionally, general practitioners (GPs) reported usability issues, with 31% avoiding the system due to incomplete records and poor interface design [86].

Outcomes achieved: Despite challenges, MHR has seen increased adoptions, with profiles populated with health data rising from 5.4 million in 2019 to 23.9 million in

2024. The system aims to enhance patient engagement, improve continuity of care and provide healthcare providers with accurate and accessible patient information. However, ongoing concerns about data security and usability indicate a need for continued investment and improvement to fully realize these benefits.

8.2 Estonian E-Health System – Estonia

Implementation Process: Estonia's e-Health system is renowned for its advanced digital infrastructure, providing citizens with a secure, centralized platform to manage their health records. Implemented using blockchain technology, the system ensures data integrity and security, allowing patients to access their medical records and monitor access history. A robust consent framework enables patients to decide which data to share and control which healthcare providers can access their information [87].

Challenges faced: Implementing blockchain technology at a national scale requires significant investment and poses technical challenges, including ensuring system interoperability and user adoption. Maintaining data privacy while allowing necessary access for healthcare providers is a delicate balance to achieve.

Outcomes achieved: Estonia's system has successfully enhanced patient empowerment and trust in public health systems. The use of blockchain technology has provided a secure and efficient model for centralized healthcare data management, serving as a benchmark for other countries [87].

8.3 Health Information Exchange (HIE) – United States

Implementation process: The Health Information Exchange (HIE) in the United States facilitates the electronic transmission of healthcare-related data among medical facilities and health information organizations [88]. It employs a decentralized data storage model, allowing patients to grant permissions on a case-by-case basis, thus maintaining individual control over data access.

Challenges faced: Implementing HIE systems across diverse healthcare providers involved challenges in standardizing data formats, ensuring interoperability and maintaining data privacy and security [89]. Additionally, achieving widespread adoption among providers requires addressing concerns about workflow integration and the costs associated with system implementation.

Outcomes achieved: HIE has improved care coordination and upheld data privacy standards, enhancing the quality and efficiency of healthcare delivery. Features such as the "break-the-glass" function provide the necessary flexibility in emergencies, while preserving patient control in non-emergency situations.

8.4 Ayushman Bharat Digital Mission (ABDM) – India

Implementation process: Launched by the Government of India, ABDM aims to create a unified digital health ecosystem by providing every citizen with a unique health ID to organize and manage their health records. It employs a consent-based data-sharing model that enables patients to determine who can access their health information via a secure mobile app or web platform [90].

Challenges faced: Implementing ABDM across a vast and diverse population poses challenges, including ensuring data security, protecting against privacy risks and achieving interoperability across different regions and healthcare providers. Bringing the digital divide and ensuring equitable access to the system are also significant concerns [91].

Outcomes achieved: ABDM has empowered patients by providing autonomy over their health data and improved healthcare continuity and interoperability across regions. However, ongoing discussions focus on refining privacy protocols to strengthen patient trust and data protection, indicating that while progress has been made, further improvements are necessary.

8.5 Aarogya Setu and Health Data Management Policy – India

Implementation process: Aarogya Setu, the Indian contact-tracing app launched during the COVID-19 pandemic, incorporated a Health Data Management Policy that focused on safeguarding user privacy. The app implemented a layered consent framework to inform users about data usage and allowed permission revocation, enhancing transparency and user control [92].

Challenges faced: The app was criticised early for its limited transparency and lack of robust privacy measures. Ensuring user trust while achieving public health objectives requires to strike a balance between data collection and stringent privacy protections [93].

Outcomes achieved: Subsequent updates have addressed initial concerns by including clear consent prompts, explicit data-sharing statements and defined data deletion protocols. These improvements reflect India's efforts to balance public health goals with individual privacy rights in digital health solutions.

8.6 eSanjeevani Telemedicine Platform – India

Implementation process: eSanjeevani is India's national telemedicine platform, providing remote healthcare access to both rural and urban populations. It employs a secure privacy model with encrypted data channels to ensure that consultation data will not be stored permanently. Each session operates under a consent-based framework, where patients agree that only necessary health information will be temporarily shared with physicians [93].

Challenges faced: The platform needs to address initial concerns about data security in telemedicine and manage public perception of privacy risks. Scalability was also a significant challenge, especially in regions with limited internet access where ensuring equitable healthcare remains a priority [93].

Outcomes achieved: eSanjeevani has become a basic tool for delivering equitable healthcare and helping reduce geographical and economic barriers to quality healthcare. The session-specific consent model and robust data encryption have set new standards for privacy in telemedicine. It now serves as a scalable telemedicine model that effectively bridges the gaps between urban medical resources and the needs of rural healthcare.

8.7 Electronic Patient Records (ePA) – Germany

Implementation process: Germany introduced the electronic patient record (ePA) in 2021 to digitize healthcare, allowing citizens to store, manage and share their health records via approved apps. Patients have complete control over their data and can decide which healthcare providers can access specific parts of their records. Apps provided by statutory health insurers serve as the primary interface for managing permissions, emphasizing ease of use and transparency [94].

Challenges faced: Launching a nationwide digital health initiative faces challenges, such as interoperability between different healthcare systems and ensuring robust cybersecurity measures. Encouraging adoption among healthcare providers and patients, while addressing privacy concerns, is a significant hurdle.

Outcomes achieved: The ePA system promotes patient autonomy by allowing individuals to manage access permissions easily. It enhances transparency and empowerment in healthcare, ensuring individuals have control over their health information. Germany’s ePA system is now a benchmark for digitized healthcare, contributing to streamlined medical services and improved patient outcomes.

9. Future directions and challenges

The future of enhancing patient autonomy in data ownership relies on continued advancements in privacy models and consent frameworks, which are essential for maintaining patient control over their healthcare data.

One promising model is blockchain technology, which ensures data security and transparency by decentralizing control and providing patients with private keys to manage access to their health data. Blockchain offers a way to securely share information while keeping the patient at the center of decisions and ensuring that data ownership remains firmly in patients' hands. This decentralized approach aligns well with regulatory frameworks such as GDPR, which emphasizes data privacy and patient rights [24]. Additionally, smart contracts within blockchain systems can automate consent processes, ensure seamless and trustworthy transactions while reducing administrative burdens. Meanwhile, this review also identifies future challenges, more specific proposals or recommendations for addressing these issues, particularly in policy development and technological innovation that will enhance its impact. For instance, tackling data breaches requires robust encryption methods and real-time monitoring systems. Addressing algorithmic biases calls for transparent training processes of AI model and regular auditing by diverse stakeholders. Furthermore, inconsistent privacy law applications could be mitigated by establishing global standards or harmonized regulations to promote universal adherence to ethical data usage. The growing complexity of managing large datasets, especially with the integration of AI into healthcare, adds another layer of difficulty in ensuring both privacy and autonomy. Technologies such as federated learning are being explored to allow data analysis without exposing sensitive information to ensure that data privacy is preserved while still contributing to healthcare advancements. Federated learning also promotes cross-institutional collaboration without compromising individual patient data [95].

As healthcare shifts towards more personalized treatments, it is crucial to develop interoperable and transparent systems that ensure patients are fully informed and have meaningful control over their data. Ethical practices must remain at the forefront, which requires stakeholders—including healthcare providers, policymakers and tech developers—to collaborate and prioritize patients' interests. Moving forward, the integration of automated consent systems, continuous updates on privacy regulations and technological tools such as adaptive AI-based consent interfaces will be essential. These advancements should be complemented by educational initiatives that empower patients with the knowledge to effectively exercise their data ownership rights. This will create a healthcare ecosystem that balances innovation, privacy and autonomy.

10. Conclusion and summary

Patient autonomy in data ownership is a cornerstone of ethical, transparent and patient-centered healthcare in the digital era. The review explored the intricate challenges and opportunities under this topic and emphasized the ethical, legal and technological dimensions of data management. Emerging technologies such as Electronic Health Records, artificial intelligence and blockchain are transforming healthcare, offering innovative ways to secure and decentralize patient data while enhancing accessibility for medical research and clinical care. Privacy models such as private, public and hybrid are crucial for balancing individual control, societal benefits and ethical use of data. Consent frameworks, such as dynamic and granular consent, empower patients to make informed decisions about their health data in real time, fostering trust and transparency. Real-world implementations, including Australia's My Health Record and Estonia's e-Health system, demonstrate the potential of patient-centered frameworks to enhance healthcare quality and innovation. Despite these advancements, challenges such as inconsistent regulations, data security risks and gaps in digital literacy persist. Addressing these issues requires a collaborative effort among stakeholders to develop adaptive, interoperable and secure systems. By prioritizing patient rights, fostering education, and aligning technological innovation with ethical principles, healthcare systems can balance individual autonomy with public health goals. This approach not only enhances trust but also establishes a sustainable foundation for advancing precision medicine and patient-centered care.

List of abbreviations

HIE: Health information exchange
EHR; EHRs: Electronic Health Records
AI: Artificial intelligence
ePR: electronic patient record
ABDM: Ayushman bharat digital mission
PDP: Personal data protection
MHR: My health record
eConsent: electronic consent
GDPR: General data protection regulation
HIPAA: Health Insurance Portability and Accountability Act.
IoT: Internet of things
CPOs: Chief privacy officers

Conflict of interests

The authors declare there is no conflicts of interests.

Funding

This review received no external funding.

Authors' contributions

All authors have accepted responsibility for the content of the manuscript and consented to its submission, reviewed all the results and approved the final version of the manuscript. Conceptualization: MRN, writing the original draft: AMK, NIW; Manuscript editing and reviewing: AMK, NIW.

References

[1] Bansal H. Negligence and Drugs in Medical Law. *Cambridge Open Engage*. 2023. doi:10.33774/coe-2023-cvw6c.

[2] Williamson L. Patient and Citizen Participation in Health : The Need for Improved Ethical Support. *The American Journal of Bioethics*. 2014; 14(6): 4-16. doi: 10.1080/15265161.2014.900139.

[3] Brall C, Schröder-Bäck P, Maeckelberghe E. Ethical aspects of digital health from a justice point of view. *The European Journal of Public Health*. 2019; 29:18-22. doi: 10.1093/eurpub/ckz167.

[4] Pal A, Saxena R, Saxena S. Artificial Intelligence Revolution in Healthcare : Transforming Diagnosis , Treatment , and Patient Care. *Asian Journal of Advances in Research*. 2024; 7(1): 241-263.

[5] Favaretto M, Shaw D, Clercq E De, Joda T, Elger BS. Big Data and Digitalization in Dentistry : A Systematic Review of the Ethical Issues. *International Journal of Environmental Research and Publich Health*. 2020; 17(7): 2495. doi: 10.3390/ijerph17072495.

[6] Lastrucci A, Pirrera A, Lepri G, Giansanti D. Algorethics in Healthcare : Balancing Innovation and Integrity in AI Development. *Algorithms*. 2024; 17(10): 342. doi: 10.3390/a17100432.

[7] Piasecki J, Cheah PY. Ownership of individual-level health data, data sharing, and data governance. *BMC Med Ethics*. 2022; 23(1):104. doi: 10.1186/s12910-022-00848-y.

[8] Prasun Kumar, Aparna Kumari (ed.). *Blockchain for Biomedical Research and Healthcare Concept, Trends, and Future Implications*. Interdisciplinary Biotechnological Advances (IBA). Singapore; Springer Nature, 2024. doi: 10.1007/978-981-97-4268-4.

[9] Campbell K, Parsi K. A New Age of Patient Transparency: An Organizational Framework for Informed Consent. *Journal of Law, Medicine & Ethics*. 2017; 45(1): 60-65. doi:10.1177/1073110517703100.

[10] Anurogo, D., Hardin La Ramba, Nabila Diyana Putri, & Ulfah Mahardika Pramono Putri. Digital Literacy 5.0 to Enhance Multicultural Education. *Multicultural Islamic Education Review*. 2023; 1(2): 109-179. doi: 10.23917/mier.v1i2.3414.

[11] Guidance WHO. Ethics and Governance of Artificial Intelligence for Health. In: *Ethics and Governance of Artificial Intelligence for Health*. 2021. p. 3-22.

[12] Mccarthy RL. Ethics and patient privacy. *Journal of the American Pharmacists Association*. 2008; 48(6): e144-155. doi:10.1331/JAPhA.2008.07144.

[13] Chiruvella V, Guddati AK. Ethical Issues in Patient

Data Ownership. *Interactive Journal of Medical Research*. 2021;10(2): e22269. doi: 10.2196/22269.

[14] Scheibner J, Ienca M, Kechagia S, Troncoso-pastoriza R, Raisaro JL, Fellay J, Vayena E. 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. *Journal of Law and Biosciences*. 2020; 7(1): lsaa010. doi: 10.1093/jlb/lsaa010.

[15] Dash S, Shakyawar SK, Sharma M, Kaushik S. Big data in healthcare : management, analysis and future prospects. *Journal of Big Data*. 2019; 54(6). doi: 10.1186/s40537-019-0217-0.

[16] Kiseleva A, Kotzinos D, De Hert P. Transparency of AI in Healthcare as a Multilayered System of Accountabilities: Between Legal Requirements and Technical Limitations. *Frontiers in Artificial Intelligence*. 2022; 5: 879603. doi: 10.3389/frai.2022.879603.

[17] Sutter E De, Meszaros J, Borry P, Huys I. Digitizing the Informed Consent Process : A Review of the Regulatory Landscape in the European Union. *Frontiers in Medicine*. 2022; 9: 906448. doi: 10.3389/fmed.2022.906448.

[18] Verreydt S, Yskout K, Joosen W, Leuven KU. Security and Privacy Requirements for Electronic Consent : A Systematic Literature Review. *ACM Transactions on Computing for Healthcare*. 2021; 2(2): 1-24. doi: 10.1145/3433995.

[19] Asswad J, Marx Gómez J. Data Ownership: A Survey. *Information*. 2021; 12(11): 465. doi: 10.3390/info12110465.

[20] Lopez LJR, Millan Mayorga D, Martinez Poveda LH, Amaya AFC, Rojas Reales W. Hybrid Architectures Used in the Protection of Large Healthcare Records Based on Cloud and Blockchain Integration: A Review. *Computers*. 2024; 13(6):152. doi: 10.3390/computers13060152.

[21] Burton LC, Anderson GF, Kues IW. Using electronic health records to help coordinate care. *Milbank Quarterly*. 2004; 82(3): 457-81. doi: 10.1111/j.0887-378X.2004.00318.x.

[22] Mello MM, Adler-Milstein J, Ding KL, Savage L. Legal Barriers to the Growth of Health Information Exchange—Boulders or Pebbles? *Milbank Quarterly*. 2018; 96(1):110-43. doi: 10.1111/1468-0009.12313.

[23] Pablo RGJ, Roberto DP, Victor SU, Isabel GR, Paul C, Elizabeth OR. Big data in the healthcare system: a synergy with artificial intelligence and blockchain technology. *Journal of Integrative Bioinformatics*. 2021;19(1): 20200035. doi: 10.1515/jib-2020-0035.

[24] Haleem A, Javaid M, Singh RP, Suman R, Rab S. Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*. 2021; 2:130-139. doi: 10.1016/j.ijin.2021.09.005.

[25] Kashyap A, Yadav A, Bajaj V, Khan Y, Arora S, Maini L. Blockchain Technology in Healthcare: The Idea and What Lies Byond. *MAMC Journal of Medical Sciences*. 2022; 8(3):187-192. doi: 10.4103/mamcjms.mamcjms_26_22.

[26] Modi KJ, Kapadia N. Securing Healthcare Information over Cloud Using Hybrid Approach. In: Panigrahi CR, Pujari AK, Misra S, Pati B, Li KC (eds). *Progress in Advanced Computing and Intelligent Engineering*. Singapore: Springer Singapore; 2019. p. 63-74.

[27] Wang X, Garg S, Lin H, Hu J, Kaddoum G, Member S, et al. Toward Accurate Anomaly Detection in Industrial Internet of Things Using Hierarchical Federated Learning. *IEEE Internet of Things Journal*. 2022; 9(10):7110-7119. doi: 10.1109/JIOT.2021.3074382.

[28] Hoofnagle CJ, Sloot B van der, Borgesius FZ. The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*. 2019; 28(1): 65-98. doi: 10.1080/13600834.2019.1573501.

[29] Rosenbloom ST, Smith JRL, Bowen R, Burns J, Riplinger L, Payne TH. Updating HIPAA for the electronic medical record era. *Journal of the American Medical Informatics Association*. 2019; 26(10):1115-1119. doi: 10.1093/jamia/ocz090.

[30] Thorogood A. Canada: will privacy rules continue to favour open science? *Hum Genet*. 2018; 137(8): 595-602. doi: 10.1007/s00439-018-1905-0.

[31] Ali M, Naeem F, Tariq M, Member S. Federated Learning for Privacy Preservation in Smart Healthcare Systems : A Comprehensive Survey. *IEEE Journal of Biomedical and Health Informatics*. 2022; 27(2): 778-789. doi: 10.1109/JBHI.2022.3181823.

[32] Gliklich RE, Leavy MB DN. *Principles of Registry Ethics, Data Ownership, and Privacy. In: Registries for Evaluating Patient Outcomes: A User's Guide*. 4th edition [Internet]. Available from: https://www.ncbi.nlm.nih.gov/books/NBK562583/.

[33] Nandimath O. Consent and medical treatment: The legal paradigm in India. *Indian Journal of Urology*. 2009; 25(3): 343-347. doi: 10.4103/0970-1591.56202.

[34] Williamson SM, Prybutok V. Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences*. 2024;14(2): 675. doi: 10.3390/app14020675.

[35] Voigt P, Bussche A. Annex I : Juxtaposition of the Provisions and Respective Recitals of the GDPR. 2017. doi:10.1007/978-3-319-57959-7.

[36] Kang M Chow, Chi C Hung, Lam K Yan. Baseline Technical Measures for Data Privacy IN the Cloud (Updated). 2023:1-86. doi: 10.13140/RG.2.2.34833.65121.

[37] Bareh CK. Reviewing the Privacy Implications of

India's Digital Personal Data Protection Act (2023) from Library Contexts. *Journal of Library & Information Technology*. 2024; 44(1): 50-58. doi: 10.14429/djlit.44.1.18410.

[38] Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Nass SJ, Levit LA, Gostin LO, editors. Washington (DC): National Academies Press (US); 2009.

[39] Bakare SS, Adeniyi AO, Akpuokwe CU. Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations. *Computer Science & IT Research Journal*. 2024; 5(3): 528-543. doi: 10.51594/csitrj.v5i3.859.

[40] Cohen IG, Mello MM. HIPAA and Protecting Health Information in the 21st Century. *JAMA*. 2018; 320(3): 231-232. doi: 10.1001/jama.2018.5630.

[41] Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*. 2022; 34(14):11475-90. doi: 10.1007/s00521-020-05519-w.

[42] Privacy D. Enhancing Data Protection in Dynamic Consent Management Systems: Formalizing Privacy and Security Definitions Zero-Knowledge Proofs. *Sensors*. 2023; 23(17): 7604. doi: 10.3390/s23177604.

[43] Albahri AS, Duhaim AM, Fadhel MA, Alnoor A, Baqer NS, Alzubaidi L, et al. A Systematic Review of Trustworthy and Explainable Artificial Intelligence in Healthcare : Assessment of Quality, Bias Risk , and Data Fusion. *Information Fusion*. 2023; 96: 156-191. doi: 10.1016/j.inffus.2023.03.008.

[44] Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent : a patient interface for twenty-first century research networks. *European Journal of Human Genetics*. 2015; 23(2):141-146. doi: 10.1038/ejhg.2014.71.

[45] Lee AR, Koo D, Kim IK, Lee E, Yoo S, Lee HY. Opportunities and challenges of a dynamic consent - based application : personalized options for personal health data sharing and utilization. *BMC Med Ethics*. 2024; 25. doi: 10.1186/s12910-024-01091-3.

[46] Aziza Chakir, Rohit Bansal, Mohamed Azzouazi (eds). Industry 5.0 and Emerging Technologies Transformation Through Technology and Innovations. *Studies in Systems, Decision and Control*. Switzerland: Springer Nature, 2024.

[47] Soni H, Grando A, Murcko A, Diaz S, Mukundan M, Idouraine N, et al. State of the art and a mixed-method personalized approach to assess patient perceptions on medical record sharing and sensitivity. *Journal of Biomedical Informatics*. 2020; 101:103338. doi: 10.1016/j.jbi.2019.103338.

[48] Tierney WM, Schwartz PH. Giving patients granular control of personal health information : Using an ethics ' Points to Consider ' to inform informatics system designers. *International Journal of Medical Informatics*. 2013; 82(12): 1136-43. doi: 10.1016/j.ijmedinf.2013.08.010.

[49] Etheredge HR. Assessing Global Organ Donation Policies : Opt-In vs Opt-Out. *Risk Management and Healthcare Policy*. 2021; 14: 1985-1998. doi: 10.2147/RMHP.S270234.

[50] Kaufman D, Bollinger J, Dvoskin R, Scott J. Preferences for opt-in and opt-out enrollment and consent models in biobank research : a national survey of Veterans Administration patients. *Genetics in Medicine*. 2012; 14(9): 787-794. doi: 10.1038/gim.2012.45.

[51] Alowais SA, Alghamdi SS, Alsuhebany N, Alqahtani T, Alshaya AI. Revolutionizing healthcare : the role of artificial intelligence in clinical practice. *BMC Medical Education*. 2023; 689: 1-15. doi: 10.1186/s12909-023-04698-z.

[52] Rahman A, Hossain S, Muhammad G, Kundu D, Muhammad G. Federated learning-based AI approaches in smart healthcare : concepts, taxonomies, challenges and open issues Data management. *Cluster Computing*. 2023; 26: 2271-2311. doi: 10.1007/s10586-022-03658-4.

[53] Dankar FK, Gergely M, Malin B, Badji R, Dankar SK, Shuaib K. Dynamic-informed consent : A potential solution for ethical dilemmas in population sequencing initiatives. *Computational and Structural Biotechnology Journal*. 2020; 18: 913-921. doi: 10.1016/j.csbj.2020.03.027.

[54] Teare HJA, Prictor M, Kaye J. Reflections on dynamic consent in biomedical research : the story so far. *European Journal of Human Genetics*. 2021; 29: 649-656. doi: 10.1038/s41431-020-00771-z.

[55] Alabdulatif A, Khalil I, Rahman MS. Security of Blockchain and AI-Empowered Smart Healthcare : Application-Based Analysis. *Applied Sciences*. 2022; 12(21): 11039. doi: 10.3390/app122111039.

[56] Alblas M, Schermer M, Vergouwe Y, Bolt I. Autonomy Challenges in Epigenetic Risk-Stratified Cancer Screening : How Can Patient Decision Aids Support Informed Consent ? *Journal of Personalized Medicine*. 2019; 9(1): 14. doi: 10.3390/jpm9010014.

[57] Wang X, Peng M, Lin H, Wu Y, Fan X. A privacy-enhanced multiarea task allocation strategy for healthcare 4.0. *IEEE Transactions on Industrial Informatics*. 2022;19(3): 2740-2748. doi: 10.1109/TII.2022.3189439.

[58] Tortorella GL, Fogliatto FS, Mac Cawley Vergara A, Vassolo R, Sawhney R. Healthcare 4.0: trends, challenges and research directions. *Production Planning & Control*. 2020; 31(15):1245-1260. doi: 10.1080/09537287.2019.1702226.

[59] Wang X, Hu J, Lin H, Liu W, Moon H, Piran J.

Federated Learning-Empowered Disease Diagnosis Mechanism in the Internet of Medical Things : From the Privacy-Preservation Perspective. *IEEE Transactions on Industrial Informatics*. 2024;19(7): 7905-7913. doi: 10.1109/TII.2022.3210597.

[60] Khan D, Jung LT, Hashmani MA. Systematic Literature Review of Challenges in Blockchain Scalability. *Applied. Sciences*. 2021; 11(20): 9372. doi: 10.3390/app11209372.

[61] Tariq MU. Revolutionizing health data management with blockchain technology: Enhancing security and efficiency in a digital era. In: *Emerging Technologies for Health Literacy and Medical Practice*. IGI Global; 2024. p. 153-175.

[62] Homoliak I, Venugopalan S, Reijsbergen D, Hum Q, Schumi R, Szalachowski P. The Security Reference Architecture for Blockchains : Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. *IEEE Communications Surveys & Tutorials*. 2021; 23(1): 341-390. doi: 10.1109/COMST.2020.3033665.

[63] Bala I, Pindoo IA, Mijwil MM, Abotaleb M, Yundong W. Ensuring Security and Privacy in Healthcare Systems : A Review Exploring Challenges, Solutions, Future Trends, and the Practical Applications of Artificial Intelligence. *Jordan Medical Journal*. 2024; 58(3).

[64] Hanna M, Pantanowitz L, Jackson B, Palmer O, Visweswaran S, Pantanowitz J, et al. Ethical and Bias Considerations in Artificial Intelligence (AI)/ Machine Learning. *Modern Pathology*. 2024; 38(3): 100686. doi: 10.1016/j.modpat.2024.100686.

[65] Hassija V, Chamola V, Mahapatra A, Singal A, Goel D, Huang K, et al. Interpreting black-box models: a review on explainable artificial intelligence. *Cognitive Compution*. 2024; 16(1): 45-74. doi: 10.1007/s12559-023-10179-8.

[66] Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. In: Artificial intelligence in healthcare. *Artificial Intelligence in Healthcare*. 2020: 295-336. doi: 10.1016/B978-0-12-818438-7.00012-5.

[67] Zhang J, Zhu H, Wang F, Zhao J, Xu Q, Li H. Security and privacy threats to federated learning: Issues, methods, and challenges. *Security Communication Networks*. 2022; 2022(1): 2886795. doi: 10.1155/2022/2886795.

[68] Yazdinejad A, Dehghantanha A, Karimipour H, Srivastava G, Parizi RM. A robust privacy-preserving federated learning model against model poisoning attacks. *IEEE Transactions on Information Forensics and Security*. 2024; 19: 6693-6708. doi: 10.1109/TIFS.2024.3420126.

[69] Bouacida N, Mohapatra P. Vulnerabilities in federated learning. *IEEE Access*. 2021; 9: 63229-63249. doi: 10.1109/ACCESS.2021.3075203.

[70] Zhu T, Ye D, Wang W, Zhou W, Philip SY. More than privacy: Applying differential privacy in key areas of artificial intelligence. *IEEE Transactions on Knowledge and Data Engineering*. 2020; 34(6): 2824-2843. doi: 10.1109/TKDE.2020.3014246.

[71] Alvim M, Chatzikokolakis K, Palamidessi C, Pazii A. Local differential privacy on metric spaces: optimizing the trade-off with utility. *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, Oxford, UK. 2018: 262-267, doi: 10.1109/CSF.2018.00026.

[72] Hu H, Salcic Z, Sun L, Dobbie G, Yu PS, Zhang X. Membership inference attacks on machine learning: A survey. *ACM Computer Survey*. 2022; 54(11s):1-37. doi: 10.1145/3523273.

[73] Stock P, Shilov I, Mironov I, Sablayrolles A. Defending against reconstruction attacks with rényi differential privacy. 2022. doi: 10.48550/arXiv.2202.07623.

[74] Ebadi H, Sands D, Schneider G. Differential privacy: Now it's getting personal. *ACM Sigplan Notice*. 2015; 50(1): 69-81. doi: 10.1145/2775051.2677005.

[75] Antunes RS, André da Costa C, Küderle A, Yari IA, Eskofier B. Federated learning for healthcare: Systematic review and architecture proposal. *ACM Transaction on Intelligent Systems and Technology*. 2022;13(4):1-23. doi: 10.1145/3501813.

[76] Abbas SR, Abbas Z, Zahir A, Lee SW. Federated Learning in Smart Healthcare: A Comprehensive Review on Privacy, Security, and Predictive Analytics with IoT Integration. *Healthcare*. 2024; 12(24): 2587. doi: 10.3390/healthcare12242587.

[77] Hassan MU, Rehmani MH, Chen J. Differential privacy techniques for cyber physical systems: A survey. *IEEE Communications Surveys & Tutorials*. 2019; 22(1):746-789. doi: 10.1109/COMST.2019.2944748.

[78] Tang J, Korolova A, Bai X, Wang X, Wang X. Privacy loss in apple's implementation of differential privacy on macos 10.12. doi: 10.48550/arXiv.1709.02753.

[79] Shahnaz A, Qamar U, Khalid A. Using blockchain for electronic health records. *IEEE access*. 2019; 7:147782-95. doi: 10.1109/ACCESS.2019.2946373.

[80] Ekblaw AC. MedRec: blockchain for medical data access, permission management and trend analysis. Massachusetts Institute of Technology; 2017.

[81] Musamih A, Salah K, Jayaraman R, Arshad J, Debe M, Al-Hammadi Y, et al. A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE access*. 2021; 9:9728-43. doi: 10.1109/ACCESS.2021.3049920.

[82] Omar IA, Jayaraman R, Salah K, Yaqoob I, Ellahham S. Applications of blockchain technology in clinical trials: review and open challenges. *Arabian Journal for Science and Engineering*. 2021; 46(4):3001-3015. doi: 10.1007/s13369-020-04989-3.

[83] Hang L, Chen C, Zhang L, Yang J. Blockchain for applications of clinical trials: Taxonomy, challenges,

and future directions. *IET Communications*. 2022; 16(20): 2371-93. doi: 10.1049/cmu2.12488.

[84] Hollo Z, Martin DE. An equitable approach to enhancing the privacy of consumer information on my health record in Australia. *Health Information Management Journal.* 2023; 52(1): 37-40. doi: 10.1177/18333583211019764.

[85] Pang PCI, McKay D, Chang S, Chen Q, Zhang X, Cui L. Privacy concerns of the Australian My Health Record: Implications for other large-scale opt-out personal health records. *Information Processing & Management*. 2020; 57(6): 102364. doi: 10.1016/j.ipm.2020.102364.

[86] Yu P, Zhang Y, Gong Y, Zhang J. Unintended adverse consequences of introducing electronic health records in residential aged care homes. *International Journal of Medical Informatics*. 2013; 82(9):772-88. doi: 10.1016/j.ijmedinf.2013.05.008.

[87] Soares B, Ferreira A, Veiga PM. The Benefits and Challenges of Blockchain Technology and eHealth Implementation in Estonia-A Literature Review. *Applied Medical Informatics*. 2023; 45(4).

[88] Menachemi N, Rahurkar S, Harle CA, Vest JR. Review The benefits of health information exchange : an updated systematic review. *Journal of the American Medical Informatics Association*. 2018; 25(9):1259-1265. doi: 10.1093/jamia/ocy035.

[89] Wu H, LaRue EM. Linking the health data system in the US: Challenges to the benefits. *International Journal of Nursing Sciences*. 2017; 4(4): 410-417. doi: 10.1016/j.ijnss.2017.09.006.

[90] Velan D, Mohandoss H, Valarmathi S, Sundar JS, Kalpana S, Srinivas G. Digital health in your hands: A narrative review of exploring Ayushman Bharat's digital revolution. *World Journal of Advanced Research and Reviews*. 2024; 23(3):1630-1641. doi: 10.30574/wjarr.2024.23.3.2762.

[91] Paliwal S, Parveen S, Singh O, Alam MA, Ahmed J. The Role of Ayushman Bharat Health Account (ABHA) in Telehealth: A New Frontier of Smart Healthcare Delivery in India. In: Arai, K (eds) *Proceedings of the Future Technologies Conference (FTC) 2023*. 2023; 2: 388-406. doi: 10.1007/978-3-031-47451-4_28.

[92] Matthan R. The Privacy Implications of Using Data REVIEW. *Journal of the Indian Institute of Science*. 2020; 100(4): 611-621. doi: 10.1007/s41745-020-00198-x.

[93] Bajpai N, Wadhwa M. National Teleconsultation Service in India: eSanjeevani OPD. ICT India Working Paper; 2021.

[94] Rau E, Tischendorf T, Mitzscherlich B. Implementation of the electronic health record in the German healthcare system: an assessment stakeholder groups. *Frontiers in Health Service*. 2024; 4: 1370759. doi: 10.3389/frhs.2024.1370759.

[95] Alsamhi SH, Myrzashova R, Hawbani A, Kumar S, Srivastava S, Zhao L, et al. Federated Learning Meets Blockchain in Decentralized Data Sharing : Healthcare Use Case. *IEEE Internet of Things Journal*. 2024;11(11): 19602-19615. doi: 10.1109/JIOT.2024.3367249.