Article

Not peer-reviewed version

Challenges and Solutions for Patient Data Protection in Large Healthcare Databases

Jasna Karacic-Zanetti *

Posted Date: 21 April 2025

doi: 10.20944/preprints202504.1650.v1

Keywords: patient data protection; healthcare databases; digital health; GDPR; HIPAA; ethical data use; cross-border data sharing

Article

Challenges and Solutions for Patient Data Protection in Large Healthcare Databases

Jasna Karacic-Zanetti

Health Diplomacy; jkaracic@unizg.hr

Abstract: The digital transformation of healthcare has led to the exponential growth of large-scale healthcare databases, raising urgent questions about the protection of sensitive patient data. This paper explores the key legal, ethical, and technological challenges involved in safeguarding personal health information across diverse systems and jurisdictions. It examines the limitations of current data protection frameworks such as the GDPR and HIPAA, particularly in the context of emerging technologies like artificial intelligence, blockchain, and federated learning. Through comparative analysis and selected case studies, the paper highlights how anonymization, interoperability, digital trust, and patient-centered governance models can be effectively combined to enhance data protection without compromising innovation. Finally, the study offers strategic recommendations for policymakers, healthcare institutions, and international networks to ensure ethical, secure, and equitable use of health data in both clinical and research settings.

Keywords: patient data protection; healthcare databases; digital health; GDPR; HIPAA; ethical data use; cross-border data sharing

1. Introduction

The digitization of healthcare systems has led to the expansion of large healthcare databases, such as electronic health records (EHRs), biobanks, and integrated data platforms (1). While these databases offer tremendous opportunities for improving healthcare quality, research, and public health monitoring, they also pose significant risks to patient privacy and data security. Sensitive health data is increasingly vulnerable to cyberattacks, unauthorized access, and misuse by third parties (2). Moreover, as artificial intelligence and cross-border health data sharing become more prevalent, ensuring strong and harmonized data protection is more important than ever (3).

In this context, healthcare institutions face growing pressure to ensure secure data storage and transmission, particularly when handling high volumes of personal health information. Advanced applications such as data analytics and machine learning are being used to enhance diagnostics, predict health conditions, and optimize treatment strategies—but they also raise critical questions about patient privacy. (4) Compliance with legal frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare organizations to implement transparent, accountable, and privacy-preserving data practices (5).

Emerging technologies such as blockchain are being explored to improve data integrity and traceability, while techniques like anonymization, de-identification, differential privacy, and federated learning are opening new pathways for secure research and innovation without compromising patient confidentiality (6). This study explores these pressing challenges and the innovative solutions being developed to strengthen patient data protection in modern healthcare systems.

1.1. Bioethics and Digital Patient Rights

The field of bioethics provides the foundational principles and ethical guidelines for managing patient rights, privacy, and the use of health data. Bioethics emphasizes respect for patient autonomy, beneficence, non-maleficence, and justice in healthcare settings. As healthcare increasingly incorporates digital tools, bioethics adapts to address issues surrounding digital patient rights, including how patient data is collected, stored, and shared. These ethical principles must evolve to ensure that patients' rights are protected in the digital landscape, balancing innovation with patient safety and dignity (7).

1.2. Information Security Theory

Information security theory focuses on safeguarding digital data and ensuring its confidentiality, integrity, and availability. In the context of healthcare, information security is critical for protecting patient data from breaches, unauthorized access, and cyber threats. This theory encompasses various technical, organizational, and procedural approaches to securing sensitive health information. It underscores the need for stringent measures to protect patient data in digital systems, thereby preventing misuse and maintaining public trust in healthcare institutions (8).

1.3. Legal Frameworks (GDPR, HIPAA)

The General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States represent key legal frameworks designed to protect patient data privacy and regulate its use (9). These laws provide a comprehensive set of rules for how personal health information should be handled, shared, and stored. GDPR focuses on data protection and individual rights within the digital ecosystem, while HIPAA sets standards for protecting patient information in the U.S. healthcare system. These legal frameworks guide institutions in maintaining compliance with privacy laws while facilitating the responsible use of health data for research and innovation (10).

1.4. Digital Trust and Patient Autonomy

In the digital age, digital trust plays a pivotal role in how patients interact with healthcare systems and share their health data. Trust is essential for patient engagement, ensuring that individuals feel confident that their data is being handled ethically and securely. Patient autonomy is a core ethical principle, reflecting the patient's right to make informed decisions about their health data and medical treatment. Digital platforms must prioritize transparency, consent, and security to foster trust and uphold patient autonomy in an increasingly data-driven healthcare environment (11).

Aim of the study:

This study aims to identify the key challenges and propose effective solutions for protecting patient data in large healthcare databases, with a focus on balancing innovation and ethical responsibility.

Research Questions:

a. What are the main challenges in ensuring data privacy in large healthcare databases?
b. How effective are current legal and technical frameworks (e.g., GDPR, HIPAA) in addressing these challenges?
c. How do different countries approach data protection in the healthcare sector?
d. Which ethical and technological solutions can enhance patient trust and data security?

2. Methodology

The methodology for this study was based on real-world findings derived from the analysis of existing practices related to data protection and patient rights, drawn from both global examples and the specific institutions notably as International Council of the Patient Ombudsman. The methodology was designed to provide both qualitative and practical insights into the balance between protecting patient privacy and enabling the use of health data for public health research, medical innovation, and AI application.

2.1. Data Collection Approach:

This study employed a mixed-methods approach, combining qualitative data and document analysis to ensure a comprehensive understanding of the challenges and opportunities in balancing patient privacy and data use in healthcare (Table 1).

a) Case Studies:

We analyzed real-world case studies from our work as Patient Ombudsmen within the International Council of Patient Ombudsmen and other relevant institutions. These case studies highlighted the ethical and operational challenges encountered in actual healthcare environments related to data protection, privacy laws, and data governance.

Case studies of healthcare institutions or digital health systems.

a. Selection Criteria: Case studies were selected based on their relevance to the use of health data in medical research, AI applications, or public health emergencies.
b. Focus Areas: Specific focus was placed on instances where data protection laws and patient consent procedures were challenged, especially during health crises or innovative research efforts.

Table 1. Overview of Key Areas in Healthcare Data Protection.

Area	Focus	Purpose/Challenge Addressed
Secure Data Storage and Transmission	Managing large volumes of health data (EHRs, medical results)	Ensure secure storage and transmission while complying with privacy laws
Privacy in Analytics & Machine Learning	Use of AI for diagnosis, prediction, treatment optimization	Protect patient privacy during complex data processing
Compliance with Regulations (GDPR, HIPAA)	Legal and ethical governance of data use	Align policies with global standards and ensure data transparency
Blockchain Technology	Decentralized data management and traceability	Enhance data security, integrity, and trust across systems
Anonymization & De-identification	Data preparation for research use	Enable safe secondary use of data without exposing personal identity
Differential Privacy	Secure statistical data analysis	Allow sharing of insights while preventing individual re-identification
Federated Learning	Distributed machine learning training	Protect sensitive data by keeping it local to healthcare institutions

b) Document and Policy Analysis:

A thorough analysis of existing documents, policies, and regulations was conducted, both at the institutional and international levels.

a. Institutional Policies: This included reviewing internal protocols for patient consent, data access, data sharing, and oversight mechanisms within the organizations involved in patient advocacy and health data protection.
b. International Guidelines: The study compared institutional policies to international frameworks and guidelines, such as GDPR, and their practical implementation in the context of patient privacy and public health research. Legal and ethical analysis (GDPR, HIPAA, national laws).

c) Literature Review:

A literature review was conducted to examine existing research and publications on the ethical use of health data, privacy regulations, and AI in healthcare. The review focused on:

a. Theoretical frameworks and ethical principles guiding data governance in healthcare.
b. Global and regional privacy laws, including GDPR, HIPAA and their impact on data sharing in medical research and public health surveillance.
c. Published case studies on the use of health data in AI applications and personalized medicine, with an emphasis on privacy concerns and ethical implications.

2.2. Data Analysis:

Data from the case studies, document analysis, and literature review were analyzed using thematic analysis to identify key themes, challenges, and best practices in managing the tension between data privacy and data use. The analysis aimed to:

a. Identify recurring ethical dilemmas related to data use in healthcare settings.

b. Understand the effectiveness of current data protection measures and patient consent protocols.
c. Assess the impact of data sharing and privacy regulations on medical innovation, AI development, and public health outcomes.

2.3. Ethical Considerations:

The study adhered to strict ethical guidelines, ensuring the privacy and confidentiality of all participants and patients. Personal data were anonymized during the analysis to protect participant identities, and as such, informed consent was not required for the use of anonymized data.

Key ethical principles followed include:

a. Privacy Protection: Ensuring that all data collected and analyzed were anonymized, preventing the identification of individuals.
b. Transparency: Clear communication about how the anonymized data would be used in the study, ensuring transparency in data governance.
c. Patient Autonomy: Although informed consent was not necessary due to anonymization, the autonomy of patients was respected through transparent processes and ethical handling of data.

2.4. Conclusion and Recommendations:

Based on the findings from the case studies, document analysis, and literature review, the study proposed recommendations for improving data governance in healthcare. These recommendations aimed to:

a. Strike a balance between data protection and data use, especially in the context of public health emergencies or AI research.
b. Propose frameworks for enhancing patient trust and transparency in data governance.
c. Suggest ways to refine patient consent processes and strengthen data security measures while fostering innovation in healthcare.

3. Results:

A. Challenges

3.1. Technical Challenges:

a. Cyberattacks, Hacking, Ransomware
The increasing reliance on digital health systems exposes patient data to a range of cyber threats, including cyberattacks, hacking, and ransomware. Healthcare institutions are prime targets for cybercriminals due to the valuable nature of the sensitive data they handle. These threats pose significant risks to data confidentiality and integrity, leading to potential breaches that can undermine public trust and safety.

b. Interoperability Issues
A major technical challenge is the lack of interoperability between different health IT systems. Healthcare organizations often use varied systems that may not communicate with each other effectively, making it difficult to share patient data across institutions or borders. This can hinder patient care, delay treatments, and prevent the seamless integration of new digital health tools, such as AI and predictive models.

c. Weak Encryption or Outdated Software
Insufficient encryption protocols and outdated software can compromise the security of health data. These vulnerabilities make systems more susceptible to breaches, data leaks, and unauthorized access, undermining patient privacy. Continuous updates and robust encryption standards are crucial to protecting patient information from emerging threats.

3.2. Legal and Regulatory Challenges:

a. Different Interpretations of GDPR
While the General Data Protection Regulation (GDPR) provides a comprehensive framework for data protection within the European Union, there are ongoing challenges regarding its interpretation. Different organizations and countries may interpret GDPR provisions in varying

ways, which can create confusion and inconsistency in the application of data protection laws, especially when dealing with international data transfers.

b. Cross-Border Data Sharing Limitations
The movement of health data across borders presents significant challenges due to varying legal frameworks and privacy regulations. For instance, the GDPR imposes stringent requirements on data transfers outside the EU, creating obstacles for global health research collaborations or multinational health organizations. This limitation can delay medical breakthroughs and limit access to vital health data.

c. Lack of Harmonization Between National Laws
The absence of harmonized data protection laws across different jurisdictions creates legal complexities when health data is shared internationally. Inconsistent national regulations can lead to uncertainty, inefficiencies, and legal risks, particularly for multinational organizations or cross-border healthcare services. This challenge highlights the need for international standards to ensure a unified approach to data governance in healthcare.

3.3. Organizational Challenges:

a. Lack of Staff Training in Data Protection
Many healthcare organizations face challenges in ensuring that their staff is adequately trained in data protection laws and best practices. Inadequate training can lead to accidental breaches, non-compliance with regulations, or mishandling of sensitive patient information. Organizations must prioritize training and capacity-building to safeguard patient data and maintain legal compliance.

b. Insufficient Internal Policies or Enforcement
Even when data protection policies exist within healthcare organizations, the enforcement and application of these policies can be weak. The lack of clear internal protocols, or insufficient monitoring and enforcement mechanisms, leaves room for errors in data management. Without strong governance, organizations may struggle to ensure that privacy protections are consistently maintained.

3.4. Ethical Challenges:

a. Informed Consent in Digital Health Systems
Obtaining informed consent in digital health systems is a major ethical challenge. Patients may not fully understand how their data will be used, shared, or stored in digital platforms. Clear, transparent, and accessible consent processes are necessary to ensure that patients are informed about the implications of their data being used in research, AI development, or other applications.

b. Patient Awareness and Digital Literacy
A significant barrier to effective data governance is the varying levels of digital literacy among patients. Many patients may not have the technical knowledge to understand the risks and benefits of digital health systems or the implications of sharing their data. Improving digital literacy and patient education is crucial to ensuring that patients can make informed decisions about their health data.

c. Concerns About Surveillance and Secondary Data Use
Ethical concerns surrounding the secondary use of health data and surveillance practices can undermine patient trust in healthcare systems. Patients may worry that their health data is being used for purposes they did not consent to, such as marketing or surveillance. Addressing these concerns requires strong safeguards, transparency, and ethical guidelines to protect patient privacy and autonomy.

Ethical Reflections on the Balance Between Data Protection and Data Use

While protecting patient privacy is a fundamental ethical and legal obligation, excessive restrictions on data access can inadvertently hinder innovation, public health research, and clinical improvements. Striking the right balance between data protection and data use remains one of the most pressing ethical challenges in digital healthcare (Table 2).

On one hand, insufficient safeguards may lead to data breaches, discrimination, or misuse of sensitive information—undermining public trust in healthcare systems and research institutions. On the other hand, overly rigid interpretations of privacy laws can restrict the use of health data in ways that delay medical discoveries or the development of more personalized and effective treatments.

This tension becomes particularly evident in the context of artificial intelligence (AI) and machine learning applications, where large volumes of data are required to develop accurate predictive models. Ethical concerns also arise in international data sharing and in public health surveillance during emergencies, where the urgency to act must be balanced against individual rights.

Patient autonomy and trust must remain at the center of any data governance model. Transparency about how data is used, patient consent processes, and mechanisms for oversight and accountability are essential components of ethically sound health data practices. Moreover, involving patients and the public in the design of data governance policies—through participatory or citizen-driven models—can help align technological progress with societal values.

Ultimately, ethical data use in healthcare must be guided not only by legal compliance but by a broader commitment to fairness, solidarity, and responsible innovation.

Table 2. Examples from practice related to the ethical challenges of balancing patient privacy with data use in healthcare.

Challenge	Context	Practical Example
Use of Data in Medical Research	Privacy laws, such as GDPR, restrict access to patient data for research purposes, which can delay medical discoveries and the development of personalized treatments.	Researchers faced challenges in accessing genetic data for personalized medicine development. Data was anonymized, and patient consent was required, which delayed the research process.
Artificial Intelligence (AI) and Machine Learning	AI and machine learning models require large datasets to develop accurate predictive models. However, data privacy concerns can restrict access to the necessary data, impacting the quality and effectiveness of AI tools in healthcare.	AI models used for predicting patient outcomes or readmissions require large datasets. Privacy laws restrict access to personal health data, which hinders the effectiveness of these models in improving healthcare delivery.
International Data Sharing and Public Health Surveillance	Public health emergencies, such as pandemics, require the urgent sharing of health data across borders. However, different countries have varying privacy laws, creating challenges in ensuring secure and legal data transfer during emergencies.	During the COVID-19 pandemic, countries shared health data to track the spread of the virus. Different countries' privacy laws created challenges in ensuring secure and legal data transfer, with concerns about data misuse.
Patient Consent and Transparency in Data Use	Ethical data governance requires transparency about how patient data is used, with a clear consent process that ensures patient autonomy. Patients must be informed and have control over their data usage.	A hospital introduced an online platform for patients to opt in for data sharing for research. Although the platform ensured transparency and patient control, some patients were reluctant due to data security concerns.
Balancing Privacy and Urgency in Public Health Emergencies	In public health emergencies, there is often an urgent need for data collection and sharing. This urgency may conflict with privacy protections, as the need to act quickly must be balanced against individual rights.	During the Ebola outbreak, mobile technology was used to track the virus' spread and send alerts. While it was effective in controlling the outbreak, concerns about privacy and the potential misuse of surveillance data arose once the emergency ended.

B. Solutions (Figure 1)

a. Implementation of Strong Security Protocols (e.g., Blockchain, Multi-Factor Authentication)
To address technical challenges, it is essential to implement strong security protocols to safeguard patient data from cyberattacks and unauthorized access. Technologies such as blockchain can offer decentralized and immutable data storage, ensuring the integrity of health data. Additionally, multi-factor authentication (MFA) can be employed to enhance access controls and prevent unauthorized access to sensitive healthcare systems.

b. Training Healthcare Staff in Data Protection and Ethical Use of AI
One of the key organizational solutions is to train healthcare staff in both data protection principles and the ethical use of artificial intelligence (AI) in healthcare. Comprehensive training programs should be implemented to ensure that staff understand the legal, ethical, and technical requirements for handling patient data. This can help minimize risks related to data breaches and ensure that AI is used responsibly to support patient care and innovation.

c. Standardization of Data Governance Practices Across Institutions
To overcome legal and regulatory challenges, there is a need for the standardization of data governance practices across institutions. Harmonizing data protection policies and practices within and between healthcare organizations can improve data interoperability, facilitate cross-border data sharing, and ensure consistent compliance with data protection laws, such as GDPR. This standardization can also enhance efficiency and reduce the risk of non-compliance.

d. Development of Patient-Centered Data Ownership Models
Ethical solutions to ensure patient autonomy include the development of patient-centered data ownership models. These models empower patients to have greater control over their health data, including the ability to decide how and with whom their data is shared. By involving patients in the decision-making process and offering clearer consent protocols, healthcare systems can build trust and respect patient rights while still enabling valuable data use for research and innovation.

e. Transparent Communication and Digital Literacy Campaigns for Patients
To address concerns about informed consent and improve digital literacy, healthcare institutions should initiate transparent communication and digital literacy campaigns for patients. These campaigns should educate patients about the digital health tools being used, the ways in which their data will be protected, and the benefits of sharing their data for research and public health purposes. Improving patient awareness will help them make informed decisions about their data and foster a sense of trust in digital healthcare systems.

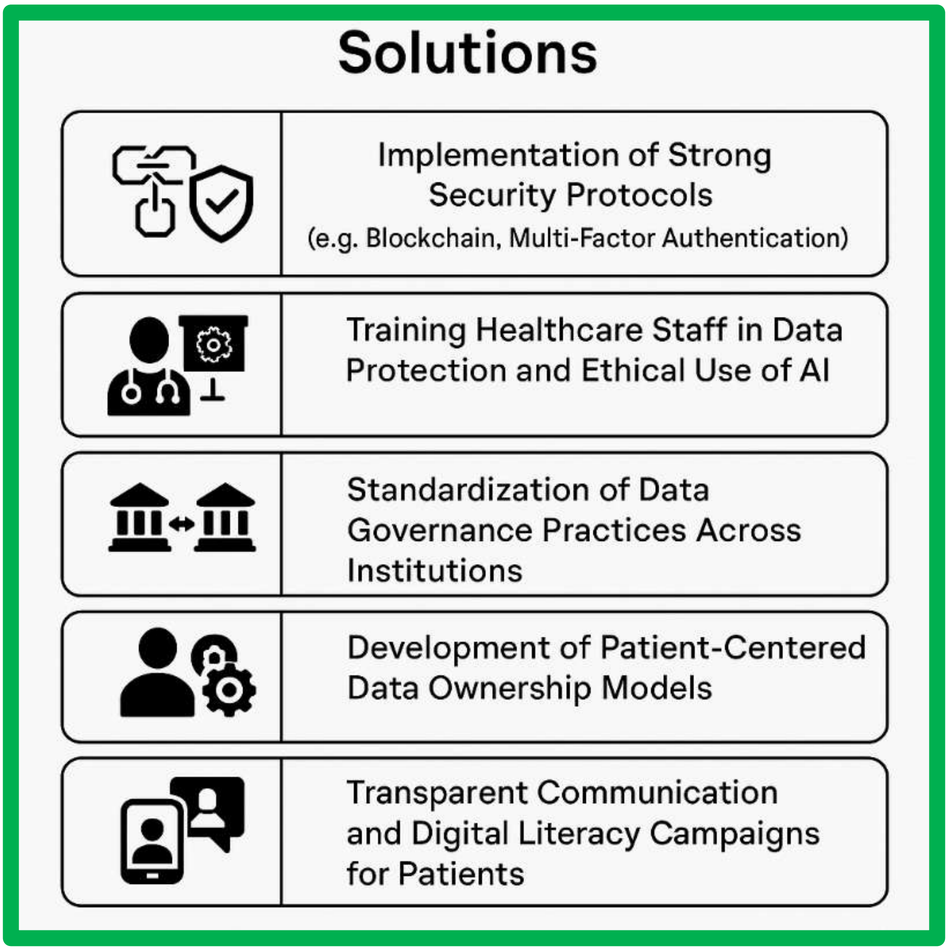

Solutions
Implementation of Strong Security Protocols
(e.g. Blockchain, Multi-Factor Authentication)
Training Healthcare Staff in Data Protection and Ethical Use of AI
Standardization of Data Governance Practices Across Institutions
Development of Patient-Centered Data Ownership Models
Transparent Communication and Digital Literacy Campaigns for Patients

Figure 1. Key Strategies for Improving Patient Data Security.

4. Discussion

The comparison of national and institutional approaches to patient data protection reveals diverse models, each with its own strengths and challenges. For instance, Estonia's e-health model stands as a global leader, integrating digital health with a focus on robust security measures, patient consent, and data interoperability across healthcare providers. This contrasts sharply with countries like Italy and the U.S., where patient data protection laws are often fragmented and the integration of digital health tools varies greatly depending on region or state. This variability exposes the complexities of creating a standardized approach to data governance on a global scale, underscoring the challenge of balancing accessibility with privacy protection (12).

A key ethical dilemma in this context is the tension between making health data accessible for research purposes and protecting personal privacy. While the use of health data is essential for advancing medical research, improving public health outcomes, and fostering innovation—especially with the rise of AI and machine learning—there is a fine line between benefiting society and overstepping privacy boundaries. Achieving this balance requires careful attention to ethical guidelines, legal frameworks, and mechanisms for patient consent, ensuring that individual rights are respected while still allowing for the responsible use of dana (13).

The growing role of artificial intelligence in healthcare further complicates the issue of data privacy. On one hand, AI has the potential to enhance healthcare delivery, personalize treatment plans, and improve patient outcomes by analyzing large datasets. On the other hand, the development of AI models relies heavily on vast amounts of patient data, raising concerns about the misuse or unauthorized access to sensitive health information. As AI technologies continue to evolve, it is essential to continuously evaluate their impact on data privacy, asking whether AI will emerge as a protector of data security or pose a threat to patient privacy if not properly regulated (14).

Finally, the importance of building public trust in digital health systems cannot be overstated. For these systems to succeed, patients must feel confident that their health data will be protected and used ethically. This trust can be fostered through transparent communication, strong data protection policies, and ensuring that patients retain control over their own information. Governments, healthcare institutions, and technology companies must collaborate to establish clear ethical guidelines and security standards to reinforce patient confidence. Without public trust, the potential of digital health systems will be severely limited, and the broader societal benefits of technological advancements in healthcare may not be fully realized (15).

Building on the discussion, the following table summarizes the key answers to the research questions addressed throughout the analysis of challenges, legal frameworks, and solutions for data privacy and security in healthcare.

- What are the main challenges in ensuring data privacy in large healthcare databases?

The main challenges include technical threats such as cyberattacks, hacking, and ransomware, which jeopardize the confidentiality and integrity of patient data. Additionally, there are issues with interoperability between different health IT systems, as many healthcare organizations use varied systems that don't communicate well with each other. This can make it difficult to share data across institutions or borders. Weak encryption protocols and outdated software further increase vulnerabilities, making patient data susceptible to breaches and unauthorized access.

- How effective are current legal and technical frameworks (e.g., GDPR, HIPAA) in addressing these challenges?

Legal frameworks like GDPR offer comprehensive protection but face challenges in their interpretation and application across different countries. This results in inconsistency and confusion, especially when dealing with international data transfers. The lack of harmonization between national laws can create legal risks and inefficiencies. While GDPR attempts to address these issues, the framework's effectiveness is hampered by varying national interpretations and cross-border sharing limitations. HIPAA in the U.S. faces similar issues, though they are not specifically addressed in the text. Therefore, while the legal frameworks provide a foundation, their effectiveness is limited by inconsistent implementation and cross-border complexities.

- How do different countries approach data protection in the healthcare sector?

Different countries approach healthcare data protection in varied ways. For example, the GDPR framework within the European Union provides a relatively unified approach but faces challenges due to differing national interpretations and the complexities of cross-border data sharing. In

doi:10.20944/preprints202504.1650.v1

contrast, countries outside the EU, like the U.S., have different frameworks (e.g., HIPAA) that may not offer the same level of consistency or protection. The text highlights the lack of harmonization between national laws, which creates additional barriers for international data sharing and complicates global health research and collaboration.

- Which ethical and technological solutions can enhance patient trust and data security?

Several solutions are proposed, both ethical and technological. Technologically, implementing strong security protocols like blockchain for decentralized data storage and multi-factor authentication for enhanced access control can significantly improve data security. On the ethical side, training healthcare staff on data protection principles and the ethical use of AI ensures that patient data is handled responsibly. Standardizing data governance practices across institutions can help improve interoperability and ensure consistent data protection. Developing patient-centered data ownership models gives patients greater control over their data, fostering trust. Lastly, transparent communication and digital literacy campaigns for patients can enhance their understanding of how their data will be used, improving trust in digital health systems and empowering patients to make informed decisions.

5. Conclusions and Recommendations

The analysis of patient data protection in digital health systems reveals several common challenges, including technical vulnerabilities (e.g., cyberattacks, weak encryption), legal complexities (e.g., inconsistent interpretations of GDPR), organizational gaps (e.g., lack of staff training), and ethical concerns (e.g., informed consent and patient autonomy). Despite these challenges, effective solutions such as the implementation of strong security protocols, staff training, standardized data governance practices, and transparent patient communication have been identified as key to improving data protection. However, significant gaps remain in achieving consistent and harmonized approaches across regions and institutions, particularly in the integration of emerging technologies like AI and the development of patient-centered data ownership models.

5.1. Practical Recommendations:

For Policymakers:

a. Need for Harmonized EU-Wide Standards: Policymakers should work towards the harmonization of data protection standards across the EU, addressing the challenges posed by varying interpretations of GDPR and creating uniform regulations that facilitate cross-border data sharing while ensuring robust privacy protection. International cooperation is also necessary to standardize privacy laws and create global frameworks for health data use.

For Hospitals and IT Departments:

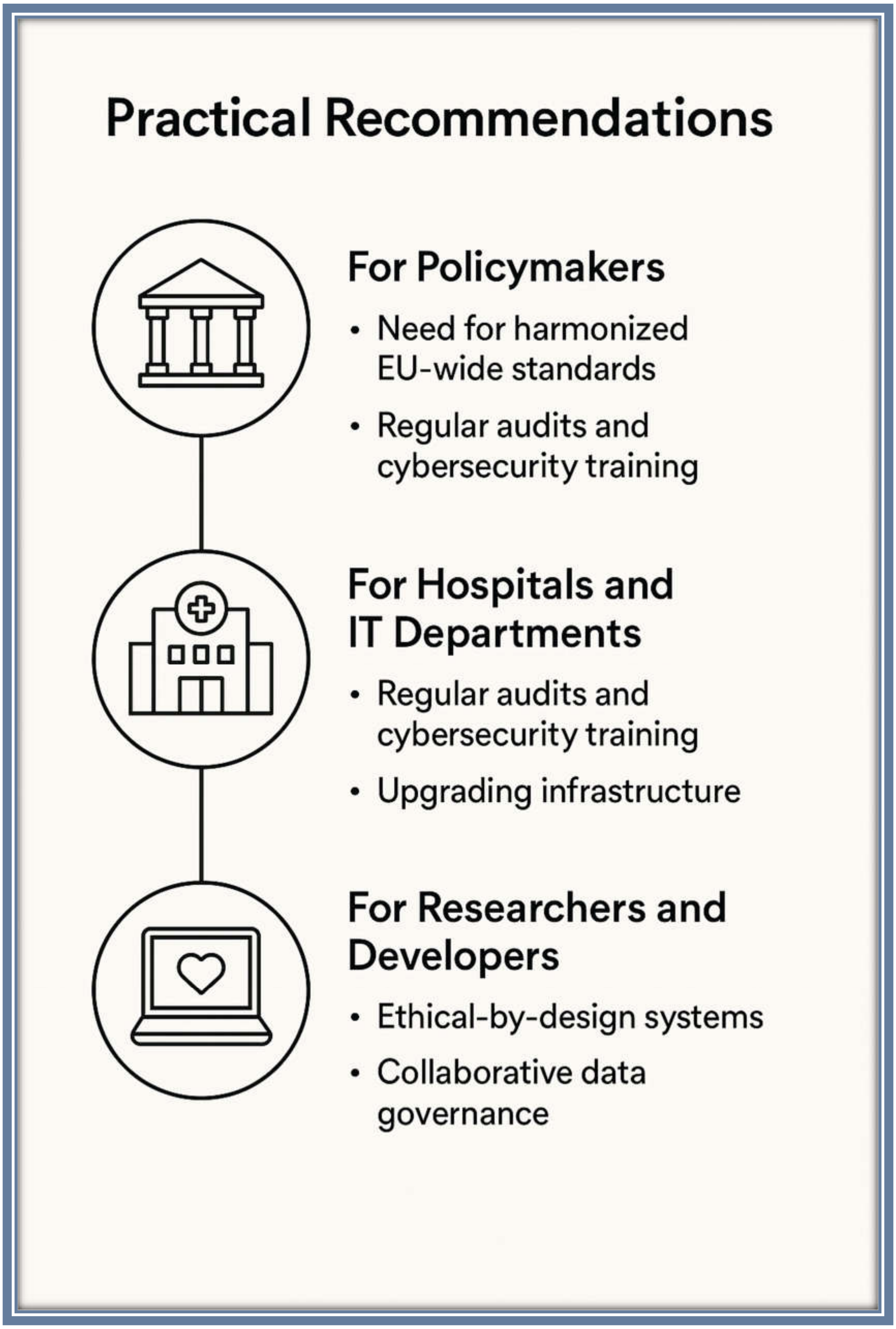
a. Regular Audits and Cybersecurity Training: Healthcare institutions must implement regular audits to assess the security of their data systems and ensure compliance with privacy regulations. IT departments should prioritize cybersecurity training for all staff members to minimize the risk of data breaches and improve internal data management practices.

b. Upgrading Infrastructure: Hospitals and IT departments should focus on upgrading outdated systems and ensuring the use of state-of-the-art encryption technologies and secure access controls to safeguard patient data.

For Researchers and Developers:

a. Ethical-by-Design Systems: Researchers and developers should embrace ethical-by-design principles when creating new digital health tools and AI applications. This includes embedding privacy protection mechanisms and transparent consent processes directly into the design of systems to ensure that patient data is handled ethically throughout the research and development phases.

b. Collaborative Data Governance: Developers should also collaborate with healthcare institutions to create data governance models that prioritize patient autonomy, transparency, and control over health data, ensuring that individuals have a meaningful say in how their data is used.



Practical Recommendations

For Policymakers

- Need for harmonized EU-wide standards
- Regular audits and cybersecurity training

For Hospitals and IT Departments

- Regular audits and cybersecurity training
- Upgrading infrastructure

For Researchers and Developers

- Ethical-by-design systems
- Collaborative data governance

Figure 2. Practical Recommendations for Enhancing Data Protection and Privacy in Digital Health Systems.

5.2. Suggestions for Further Research:

a. Emerging Technologies: Future research should focus on the ethical implications and potential of emerging technologies in digital health, such as blockchain for secure data storage, AI for predictive healthcare models, and wearable devices that collect continuous health data. Research should explore how these technologies can be integrated into existing systems without compromising patient privacy.

b. Patient Engagement Strategies: There is a need for further studies on patient engagement strategies in digital health systems, particularly how patients can be empowered to make informed decisions about their data and the ways in which digital literacy can be improved across diverse populations. Research into participatory models for patient consent and data ownership would also be valuable in aligning technology with patient rights and public trust.

References

1. Shabani M, Marelli L. Re-identifiability of genomic data and the GDPR. EMBO Rep. 2019;20(6):e48316.
2. Organisation for Economic Co-operation and Development (OECD). Health Data Governance: Privacy, Monitoring and Research. Paris: OECD Publishing; 2021.
3. Wang Y, Kung L, Byrd TA. Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. Technol Forecast Soc Change. 2018;126:3–13.
4. Rieke N, Hancox J, Li W, Milletari F, Roth HR, Albarqouni S, et al. The future of digital health with federated learning. NPJ Digit Med. 2020;3:119.
5. Glicksberg BS, Johnson KW, Shameer K, Dudley JT. Data science approaches to precision medicine. Curr Cardiol Rep. 2018;20(12):139.
6. Engelhardt MA. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Technol Innov Manag Rev. 2017;7(10):22–34.
7. Karacic Zanetti J, Nunes R. To Wallet or Not to Wallet: The Debate over Digital Health Information Storage. Computers. 2023;12(6):114. doi:10.3390/computers12060114.
8. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. Int J Internet Enterp Manag. 2010;6(4):279–314.
9. Voigt P, Von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. 1st ed. Cham: Springer International Publishing; 2017.
10. U.S. Department of Health and Human Services (HHS). Summary of the HIPAA Privacy Rule [Internet]. Washington, DC: HHS; 2003 [cited 2025 Apr 10]. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
11. Nebeker C, Torous J, Bartlett Ellis RJ. Building the case for actionable ethics in digital health research supported by artificial intelligence. *BMC Med*. 2019;17(1):137.
12. Kluge EHW, Ruotsalainen P. A comparative study of health information privacy in Europe: An illustration of the influence of European Union and national policies. Int J Med Inform. 2012;81(12):834–41.
13. Mittelstadt BD, Floridi L. The ethics of big data: Current and foreseeable issues in biomedical contexts. Sci Eng Ethics. 2016;22(2):303–41.
14. Morley J, Floridi L. The limits of empowerment: How to reframe the role of mHealth tools in the healthcare ecosystem. Sci Eng Ethics. 2020;26(3):1159–83.
15. Price WN, Cohen IG. Privacy in the age of medical big data. Nat Med. 2019;25(1):37–43

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.