computers

MDPI

*Review*

# To Wallet or Not to Wallet: The Debate over Digital Health Information Storage

**Jasna Karacic Zanetti [1,2,*] and Rui Nunes [2,3,*]**

[1] University of Zagreb, 10000 Zagreb, Croatia
[2] International Council of the Patient Ombudsman, Health Diplomacy Unit, 1000 Brussels, Belgium
[3] Center of Bioethics of the Faculty of Medicine, University of Porto, 4200-319 Porto, Portugal
[*] Correspondence: jkaracic@unizg.hr (J.K.Z.); ruinunes@med.up.pt (R.N.)

**Abstract:** The concept of the health wallet, a digital platform that consolidates health-related information, has garnered significant attention in the past year. Electronic health data storage and transmission have become increasingly prevalent in the healthcare industry, with the potential to revolutionize healthcare delivery. This paper emphasizes the significance of recognizing and addressing the ethical implications of digital health technologies and prioritizes ethical considerations in their development. The adoption of health wallets has theoretical contributions, including the development of personalized medicine through comprehensive data collection, reducing medical errors through consolidated information, and enabling research for the improvement of existing treatments and interventions. Health wallets also empower individuals to manage their own health by providing access to their health data, allowing them to make informed decisions. The findings herein emphasize the importance of informing patients about their rights to control their health data and have access to it while protecting their privacy and confidentiality. This paper stands out by presenting practical recommendations for healthcare organizations and policymakers to ensure the safe and effective implementation of health wallets.

**Keywords:** e-health; health wallet; digital health; GDPR; patient identification and authentication; ethics; data privacy and access

check for updates

**Citation:** Karacic Zanetti, J.; Nunes, R. To Wallet or Not to Wallet: The Debate over Digital Health Information Storage. *Computers* **2023**, *12*, 114. https://doi.org/10.3390/computers12060114

Academic Editors: Tayeb Lemlouma, Yevgeniya Kovalchuk, Sébastien Laborie and Abderrezak Rachedi

Received: 4 April 2023
Revised: 23 May 2023
Accepted: 25 May 2023
Published: 28 May 2023

**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

In today's digital age, e-health data has become an essential part of healthcare services. E-health data comprises health-related information that is electronically stored and transmitted through various electronic devices and networks, including medical records, diagnostic results, and patient information [1]. Digital health is a rapidly growing field that promises to revolutionize healthcare by providing innovative solutions to long-standing problems. In recent years, there has been a significant shift towards digital health information storage, with the increasing adoption of electronic health records [EHRs] and other digital health technologies. With the rapid advancement of technology, it is crucial to recognize the ethical implications of digital health and ensure that ethical considerations are at the forefront of this field's development [2]. Health information storage refers to the secure electronic storage of personal health records, while a health wallet is the concept of **an integrated** digital platform that allows individuals to manage and control their own health information [3].

The idea behind the health wallet is to empower individuals to take control of their health by giving them access to their medical records, lab results, prescription information, and other health-related data. The purpose of a health wallet is to provide individuals with more control over their own health information, making it easier for them to access and share their information with healthcare providers, family members, or other relevant parties [4]. Some health wallets may also allow for the integration of data from wearable devices and other health-related apps, providing a more comprehensive view of an individual's health. The health wallet concept also aims to make it easier for individuals to share their health information with healthcare providers, researchers, and other relevant parties. This can improve the coordination of care and ultimately lead to better health outcomes [5].

Several companies and organizations are currently developing health wallets, and some governments are exploring the concept as part of their national healthcare strategies [6]. One that piqued interest is The Electronic Identification, Authentication, and Trust Services (eIDAS) Regulation, which is legislation adopted by the European Union (EU) in 2014 that provides a framework for secure and reliable electronic transactions across the EU [7].

We have investigated health wallets' specific features and capabilities, which may vary depending on the provider. Still, they generally involve a secure, encrypted platform for storing and accessing health-related data.

Cross-border identity verification also plays a critical role in patient identification and authentication. In cross-border healthcare, patients may receive medical treatment from healthcare professionals who are unfamiliar with their medical history, making accurate identification and authentication of patients even more crucial. Verifying the identity of patients is essential to ensure that they receive the right treatment and medication, prevent medical errors, and protect patients' privacy and confidentiality [8].

While this has many potential benefits, such as improving patient care and reducing medical errors, it also raises concerns about data security, privacy, and access. As such, the debate over digital health information storage has become a hot topic in the healthcare industry, pointing out the advantages and practicability of personalized medicine, reducing medical errors, and empowering patients while protecting privacy.

This topic is critical for understanding the future of healthcare and the implications of adopting digital health technologies. One of the major aims of this work was to explore the arguments for and against digital health information storage and to understand the potential impact of these technologies on healthcare delivery and patient outcomes. Our research aimed to find a solution for the challenging problem of ethical considerations in developing digital health technologies like health wallets.

One novel aspect of this paper is its focus on the potential impact of health wallets on patient rights, particularly the Right to Free Choice and the Right to Privacy and Confidentiality. By highlighting these issues, this paper adds to the growing body of literature on the ethical implications of digital health technology and encourages healthcare providers and policymakers to consider the broader societal implications of these technologies.

This study contributes by providing insights into the ethical considerations, challenges, and potential benefits of digital health information storage.

This paper offers a unique perspective on health wallet implementation, emphasizing a risk-based approach to identify and prioritize security threats while highlighting the significance of patient rights, data security, system interoperability, cross-border healthcare challenges, data accuracy, and standardization, thereby enhancing the understanding of the future of healthcare and the implications of digital health technologies.

This approach provides a practical framework for healthcare organizations to allocate resources effectively and efficiently, ensuring that patient data remain secure and private.

## 2. Problem at a Glance

The relationship between doctors and patients is built on mutual trust and respect, which are essential components of effective healthcare. The quality of the relationship and trust between a doctor and a patient can significantly influence the patient's treatment plan and overall health outcomes. When patients trust their doctors, they are more likely to adhere to treatment plans, follow medical advice, and engage in shared decision-making. Trust and good communication between doctors and patients can also improve patient satisfaction and lead to better clinical outcomes. The trust between doctors and patients is built on medical ethics, and when it comes to making decisions about giving access to personal health records, confidence is essential.

### *2.1. Ethics*

Medical ethics provides the framework for ethical behavior in healthcare and establishes the standards for appropriate conduct and decision-making [9]. Doctors who follow ethical principles and guidelines are more likely to earn their patients' trust and confidence as they demonstrate a commitment to professionalism, integrity, and patient-centered care. Medical ethics plays a key role in addressing ethical issues and conflicts that can arise from data sharing and health wallets. Medical ethics is a complex and evolving field that deals with a wide range of ethical dilemmas and issues related to healthcare. It also involves developing and applying ethical standards and guidelines to ensure that healthcare practices are conducted in a manner that is consistent with professional and societal expectations. Medical ethics aims to promote respect for patients' autonomy, dignity, and well-being while balancing competing interests and values.

One of the primary ethical considerations in digital health is the protection of patient privacy and data protection in accordance with the universal right to healthcare. The use of electronic health records, health apps, and other digital technologies requires that sensitive patient data be collected and stored securely [10].

It is essential to ensure that patients have control over their data, including the ability to access and review their information, correct inaccuracies, and determine who has access to their data and that it is not used or shared without their consent, as well to ensure that patient data is securely stored and that data is only accessed and used for its intended purpose [10]. This control on personal information also includes the right to be forgotten, meaning that any person has the ethical and legal right to erase personal health information from the digital system, as long as the rights of third parties are not unethically compromised [11].

The development of digital health technology must, therefore, include strong privacy protections and safeguards to prevent data breaches.

Another important ethical consideration is the potential for digital health technologies to exacerbate existing health disparities. It is critical to ensure that the benefits of digital health are accessible to everyone, regardless of their socioeconomic status or geographic location. Digital health should be designed with an equity lens and should strive to reduce, rather than perpetuate, existing health disparities [12].

### *2.2. Data Privacy and Access*

While e-health data has many benefits, its use can also affect two crucial patient rights: the Right to Free Choice and the Right to Privacy and Confidentiality [13].

The Right to Free Choice is a fundamental right of every patient to choose their healthcare provider and receive treatment that aligns with their personal values and preferences. E-health data can affect this right because it may limit a patient's ability to choose a provider or receive the type of treatment they prefer. For example, if a patient's medical records indicate that they have a pre-existing condition, some insurance providers may deny them coverage or only offer limited treatment options, which may limit the patient's ability to choose the best care for themselves [14]. The Right to Privacy and Confidentiality is another essential patient right that can be affected by using e-health data. This right ensures that patients have control over their health-related information, and healthcare providers cannot disclose it without their explicit consent. E-health data can affect this right because it is often stored on electronic devices that are vulnerable to hacking and unauthorized access. Additionally, some healthcare providers may share a patient's health-related information with other providers or third parties without their consent, which can compromise their privacy and confidentiality [15]. The problem is even more complex because some digital infrastructures are geographically localized in countries with different laws and different ethical backgrounds.

One of the main problems with digital health, when all healthcare professionals can see the history of all treatments in the same hospital, is the issue of patient privacy and data protection. While having a shared electronic health record can improve the coordination and quality of care, it also raises concerns about who has access to a patient's sensitive health information and how it is being used [16]. Inappropriate access to patient health records can lead to breaches of patient confidentiality, which can have serious consequences for patients and healthcare providers. Additionally, if patient data is not properly secured, it may be vulnerable to cyberattacks and data breaches, which can compromise the privacy and security of a patient's health information [17].

The abuse of patient data in hospital computer systems can have serious consequences, including breaches of patient privacy, discrimination, and other harms. Such abuse may occur if hospital staff or others with access to patient data use it for purposes beyond those authorized by the patient or for their own personal gain.

To prevent such abuses of patient data, hospitals and healthcare providers must have strong data protection policies in place, including secure computer systems and appropriate access controls to limit access to sensitive patient information. Staff should receive regular training on the importance of protecting patient data and the consequences of breaching privacy rules, namely from a criminal perspective.

One example of abuse of patient data is identity theft, where personal and medical information is stolen and used for fraudulent purposes. In some cases, patient data may also be used to discriminate against patients based on their medical history or other characteristics, such as race or gender [18].

Another potential issue is the sale or unauthorized sharing of patient data to third parties, such as insurance companies, marketers, or other healthcare providers. This can result in patients being targeted for marketing or other purposes without their knowledge or consent.

Furthermore, there may be practical challenges associated with implementing a shared electronic health record system, such as ensuring that all healthcare professionals have access to the system and are trained in how to use it effectively. There may also be challenges related to standardizing data and ensuring that information is entered accurately and consistently.

Overall, while a shared electronic health record system can have many benefits, including improved coordination of care and better outcomes for patients, it is important to carefully consider the potential risks and challenges associated with such a system, particularly in terms of patient privacy and data protection [19]. Healthcare providers and organizations must implement robust security measures and ensure that all users of the system are trained in the best practices for maintaining patient confidentiality and protecting patient data.

### *2.3. Cross Border*

The use of digital health technologies in cross-border healthcare presents several challenges and problems that need to be addressed to ensure that patients can benefit from these technologies while also protecting their safety, privacy, and rights [20] (Table 1). Addressing these challenges will require collaboration and coordination between different countries, healthcare providers, companies, and regulators.

However, both the approval of the General Data Protection Regulation ((GDPR) [21]) as well as the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space [22], are huge steps for a more comprehensive and harmonized data space, at least in the European Union.

### *2.4. Data Security and Accuracy*

One of the biggest concerns with digital health information storage is data security. Medical records contain sensitive information that can be used for identity theft or fraud.

Protecting this data from cyber-attacks and breaches is crucial, and healthcare providers must implement strong security measures to ensure patient privacy.

**Table 1.** Challenges and problems associated with the use of digital health in cross-border healthcare.

| | |
|---|---|
| Fragmented regulatory environment: | The regulatory environment for digital health technologies is fragmented across the EU, with different countries having different rules and regulations for the use of digital health technologies. This can make it difficult for companies and healthcare providers to navigate the regulatory landscape and comply with all the necessary requirements. |
| Interoperability issues: | Digital health technologies often rely on interoperability to function effectively, but different countries and healthcare systems may have different technical and data standards. This can create challenges for sharing data and information across borders and can limit the effectiveness of digital health technologies. |
| Privacy and data protection: | The use of digital health technologies raises important issues around privacy and data protection. Patients' personal health information is often sensitive and must be handled carefully, but different countries have different legal requirements and approaches to privacy and data protection. This can make it difficult to ensure that patient data is protected when it is shared across borders. |
| Reimbursement and funding: | Different countries have different reimbursement and funding systems for healthcare services and technologies, which can make it difficult for companies to commercialize and sell digital health technologies across borders. |
| Patient safety and quality of care: | The use of digital health technologies in cross-border healthcare can raise concerns about patient safety and the quality of care. Without proper regulations and standards in place, there is a risk that patients may receive suboptimal care or be exposed to safety risks. |

Health data must be accurate and up-to-date to be useful. However, errors can occur during data entry, which can affect the accuracy of the data. Data quality can be affected by the lack of standardization in data collection and storage across different systems and providers. Quality assurance programs must be implemented by health organizations to guarantee appropriate levels of security and accuracy.

### *2.5. System Complexity and Interoperability*

Digital health information storage systems can be complex and difficult to use, especially for healthcare providers who are not familiar with the technology. This can lead to errors and frustration and may prevent some providers from using the systems to their full potential. It follows that programs on digital health targeted at healthcare professionals should be implemented, namely for the acquisition of digital skills and inclusion.

Digital health information storage systems are often not interoperable, meaning they cannot easily share information with other systems. This can lead to the fragmentation of health data and make it difficult for healthcare providers to access complete and accurate patient information.

## 3. Discussion

Digital health, e-health, and health wallets are rapidly growing fields that promise to revolutionize healthcare by providing innovative solutions to long-standing problems.

While the use of health wallets is still relatively new, they have the potential to significantly improve the efficiency and effectiveness of healthcare delivery while also improving patient empowerment and engagement. However, it is important to note that the security and privacy of personal health information should be carefully managed and protected in the context of health wallets [23]. To overcome challenges, there is a need for increased collaboration between healthcare providers, policymakers, patients, and other stakeholders. This collaboration can help to identify and address the barriers to health data-sharing while also ensuring that patient privacy and data protection are maintained. Additionally, technological solutions such as common data formats, standards and protocols, and digital platforms can help to facilitate health data-sharing. This suggests that collaborations between healthcare providers and policymakers can help overcome barriers to health data-sharing through technological solutions, such as common data formats, standards, and digital platforms.

The use of data in healthcare has the potential to revolutionize the industry and improve patient outcomes in numerous ways. By analyzing patient data such as genetics, lifestyle, and medical history, healthcare providers can create personalized treatment plans for each patient, which is a key opportunity for personalized medicine and for the development of precision medicine. By analyzing large amounts of data, namely stratified genetic information, healthcare providers can identify trends and patterns that may signal potential health risks in specific patient populations. This information can be used to develop targeted disease prevention and early detection strategies. To improve operational efficiency by analyzing data on patient flow, resource utilization, and supply chain management, healthcare organizations can identify areas where they can increase efficiency and reduce costs. In clinical research, by leveraging data from electronic health records [EHRs] and other sources, researchers can conduct large-scale studies that generate new insights and advance medical knowledge. For improving patient outcomes by collecting and analyzing data on patients, healthcare providers can identify areas for improvement and implement evidence-based practices that improve patient care.

Privacy and data protection are crucial aspects of digital health, particularly when it comes to managing health information in hospital computer systems. It is important to ensure that patients' health data is securely stored and managed in compliance with relevant data protection regulations, such as the EU General Data Protection Regulation.

Patients should also be informed about their rights to control their own health data and have access to it, as well as the potential risks associated with sharing their data with others. By providing patients with greater control over their health data and ensuring that hospitals and healthcare providers protect patient privacy and prevent data abuse, we can help to build trust in the digital health system and improve patient outcomes [24].

Our data showed that while health wallets hold promise for improving healthcare access and outcomes, there are still challenges to address, such as ensuring data accuracy and reliability and patient trust in the technology.

Hospital computer systems should have robust security protocols in place to prevent unauthorized access to patient data, as well as secure methods for transferring data between different systems or healthcare providers. Patient data should be encrypted during transmission and storage to ensure that it remains confidential and secure.

It is interesting to note that patients should have control over their own health data, including the ability to access and review their information, correct inaccuracies, and determine who has access to their data. Hospitals and healthcare providers should obtain explicit consent from patients before collecting or sharing their data and ensure that patients understand how their data will be used.

Healthcare providers also have a responsibility to ensure that patient data is only used for its intended purpose and that data is not shared or used inappropriately. This is particularly important when investigating how the regular monitoring of hospital computer systems and implementing data access controls limit access to patient data to only those who need it to provide healthcare services [25]. Eventually, stringent national and EU legislation is necessary so that patient rights are not violated.

Ensuring the privacy and security of patient data in digital health systems is critical to maintaining patient trust and confidence and improving the overall quality of healthcare delivery.

Without effective cross-border identity verification, it may be difficult to ensure that only authorized individuals can access sensitive medical information and provide healthcare services. This can result in medical errors, security breaches, and risks to patient safety and privacy. Therefore, it is important to have robust cross-border identity verification processes in place to safeguard the integrity of the healthcare industry and protect the well-being of patients.

Nevertheless, we found that there are still challenges that need to be addressed for health wallets to become widely adopted. These include addressing interoperability issues, ensuring data accuracy and reliability, and ensuring patient trust in the technology and the healthcare system as a whole. It remains an ongoing challenge to answer: what to do if Information and Technology [IT] systems or companies are unreliable; what if they close the company and the data is no longer available?

We have shown that health wallets have the potential to transform the way healthcare is delivered and empower patients to take control of their health data. As the technology continues to evolve and improve, it will be important for healthcare providers and policymakers to work together to ensure that health wallets are implemented in a safe, secure, and effective manner.

The solutions presented in this paper contribute to the body of scientific knowledge by emphasizing the ethical implications of digital health technologies and prioritizing ethical considerations in the development of the health wallet concept.

Balancing patient privacy and patient safety for sharing e-health data requires careful consideration of several factors, including the sensitivity of the data, the potential benefits and risks of sharing the data, and the legal and ethical requirements for data protection. One possibility is to adopt a principle-based approach to medical ethics. This involves identifying and applying ethical principles, such as respect for patient autonomy, beneficence, non-maleficence, and justice, to guide decision-making in the context of sharing e-health data. Respect for patient autonomy means that patients have the right to control their personal health information and decide who has access to it [26]. In the context of sharing e-health data, this principle requires obtaining the patient's informed consent before sharing their data with third parties. Patients should be informed about the purpose of data sharing, who will have access to their data, and the potential risks and benefits of sharing their data [27]. Beneficence and non-maleficence require healthcare providers to act in the best interests of their patients and to avoid harm. These principles require balancing the potential benefits of data sharing, such as improved healthcare outcomes, against the potential risks, such as breaches of patient privacy. Justice requires that healthcare resources be distributed fairly and equitably and that no patient is unfairly disadvantaged by the sharing of their data. Another possibility is to adopt a risk-based approach. Under certain assumptions, this can be construed as assessing the potential risks of data sharing, such as the risk of unauthorized access, data breaches, and misuse of patient data, and implementing appropriate security measures to mitigate those risks [5]. Examples of security measures include data encryption, access controls, regular security audits, and also passing robust legislation in the area.

### *3.1. Challenges of Digital Health in the Future*

Technical interoperability: Health data is often stored in different formats and in various IT systems, making it difficult to share and combine data between different healthcare providers. This lack of interoperability can result in incomplete or fragmented data sets, limiting the usefulness of the data for research and healthcare delivery.

Data ownership: Health data is typically owned by the patient, but healthcare providers also collect and use this data. The question of who owns the data and who has the right to access and use it can be a contentious issue, particularly when it comes to sharing data between different healthcare providers or across national borders. The creation of huge, organized collections of big data and lake data should also be regulated.

Cultural differences: The cultural and social norms of different countries can also create challenges to health data sharing. For example, some EU member states have a strong cultural emphasis on privacy, which can create resistance to data sharing, while others may be more willing to share data for the common good.

Trust and transparency: Trust and transparency are key to enabling health data sharing, and there are concerns among some individuals and groups about the potential misuse of health data or the loss of control over their data. Building trust and ensuring transparency around data-sharing practices is critical to overcoming these challenges.

Key findings that emerge from these challenges include the concept of the health wallet, ethical considerations in digital health, potential benefits and concerns of digital health information storage, a risk-based approach for implementing health wallets, the impact of health wallets on patient rights, challenges in cross-border healthcare, data security and accuracy, and system complexity and interoperability. These findings highlight the importance of addressing ethical implications, such as patient rights and privacy, in the development and implementation of digital health technologies **as well as the need to increase health literacy in this area.** Furthermore, they emphasize the need for robust data security measures, accurate information storage, and seamless interoperability across healthcare systems. By understanding and addressing these key findings, we can enhance the future of healthcare and ensure the responsible and effective use of digital health technologies.

### *3.2. Recommendation*

Healthcare organizations can improve the safety and security of e-health data, which can enhance patient trust and confidence in electronic healthcare services (Figure 1), by implementing the following recommendations:

1. Implement strong data security measures: Healthcare organizations should implement strong security measures to protect e-health data from unauthorized access, theft, and cyberattacks. This may include encryption, multi-factor authentication, and regular security audits;
2. Educate staff on best practices: Healthcare staff should be trained on best practices for handling e-health data, including how to securely store, transmit, and access electronic records. This can help prevent human errors and data breaches;
3. Ensure compliance with regulations: healthcare organizations should ensure compliance with regulations and standards, such as the Health Insurance Portability and Accountability Act [HIPAA] and the General Data Protection Regulation [GDPR], to protect patient privacy and confidentiality;
4. Regularly update software and systems: healthcare organizations should keep their software and systems up to date with the latest security patches and updates to reduce the risk of vulnerabilities and data breaches, namely in the face of a sudden rise or artificial intelligence;
5. Foster a culture of safety and transparency: healthcare organizations should create a culture of safety and transparency around e-health data use, including encouraging staff to report any suspected security incidents or breaches [whistleblowing];
6. Use a risk-based approach: Healthcare organizations should use a risk-based approach to identify potential security threats and prioritize their response based on the level of risk. This can help allocate resources more effectively and efficiently.

These recommendations contribute to scientific knowledge by addressing the challenges associated with e-health data security. Other experts can use these results to inform healthcare research and development and improve the safety and security of electronic healthcare services.

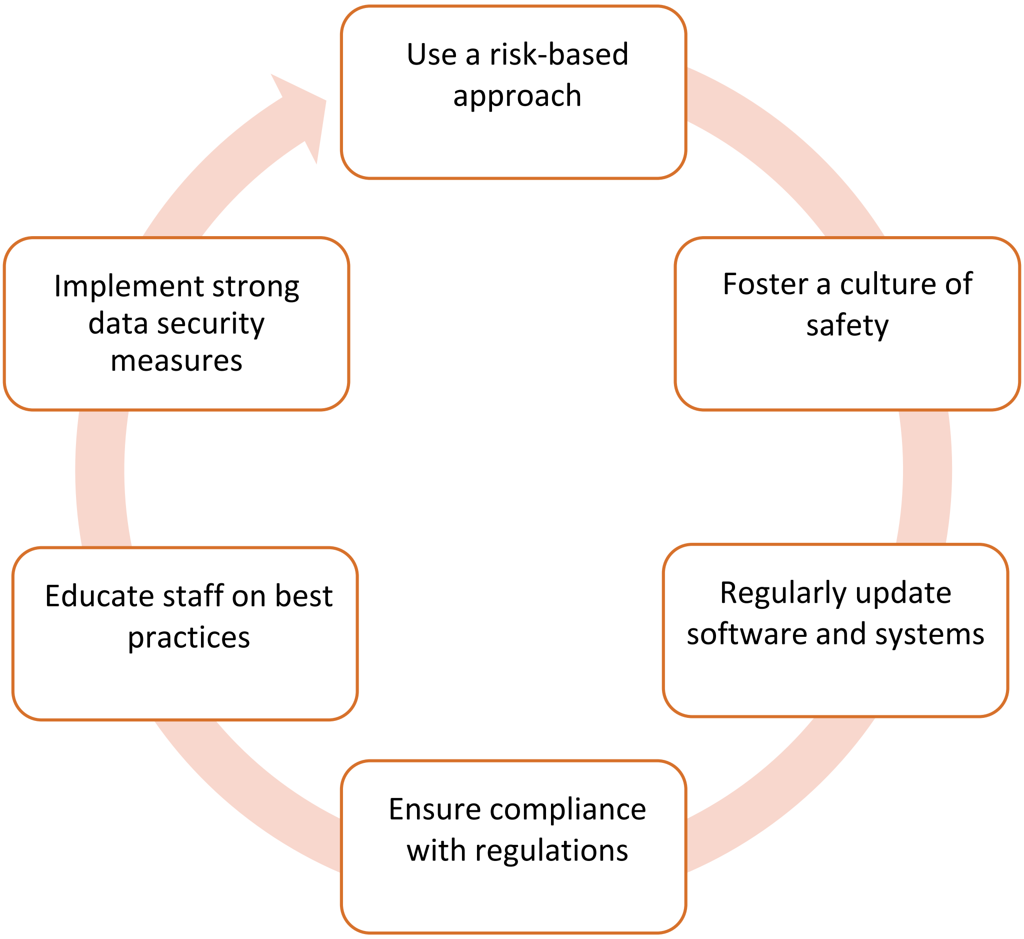
Use a risk-based approach
Foster a culture of safety
Regularly update software and systems
Ensure compliance with regulations
Educate staff on best practices
Implement strong data security measures

**Figure 1.** Recommendations for improving safety when using e-health data.

## 4. Conclusions

This study suggests that the development of digital health technology holds great promise for the future of healthcare. It is essential to recognize the ethical implications of these technologies and ensure that ethical considerations are at the forefront of development. We must strive to protect patient privacy, ensure equitable access, and avoid perpetuating existing biases in healthcare. By allowing patients to control access to their health data, health wallets can help improve data privacy and security, which casts a new light on enabling patients to take a more active role in their healthcare. Our data indicate that health wallets also have the potential to improve healthcare outcomes by facilitating the exchange of health data between patients and healthcare providers. This can lead to more informed and personalized healthcare decisions, as well as more efficient and effective healthcare delivery.

Our data suggest that we still have a long way to go to fully realize the potential benefits of health wallets and digital health technology. While these technologies hold promise for improving healthcare access and outcomes, further research is needed to ensure their effectiveness and security. It will be important that future research investigates how digital health technology can impact clinical trials and their outcomes.

**Author Contributions:** Conceptualization, J.K.Z.; methodology, J.K.Z. and R.N.; software, J.K.Z. and R.N.; validation, J.K.Z. and R.N; formal analysis, J.K.Z. and R.N.; investigation, J.K.Z. and R.N.; resources, J.K.Z. and R.N.; data curation, J.K.Z. and R.N.; writing—original draft preparation, J.K.Z.; writing—review and editing, R.N.; visualization, J.K.Z. and R.N.; supervision, R.N. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** All data were presented in the main text.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Topol, E. *The Topol Review: Preparing the Healthcare Workforce to Deliver the Digital Future*; Department of Health and Social Care: London, UK, 2019.
2. McCarthy, J.A.; DeRenzi, B. Ethical Considerations in Digital Health. *Curr. Opin. Cardiol.* **2021**, *36*, 509–513.
3. Wollaston, L. The Health Wallet: A Digital Tool to Empower Individuals in Managing Their Health-Related Information. *J. Med. Internet Res.* **2019**, *21*, e13147.
4. Ammenwerth, E.; Duftschmid, G.; Gall, W.; Hackl, W.O.; Hoerbst, A.; Janzek-Hawlat, S.; Jeske, M.; Jung, M.; Woertz, K. The future of electronic health records: A commentary. *J. Med. Syst.* **2020**, *44*, 204.
5. Bauer, S.; Perkmann, T.; Muaremi, A.; Grünerbl, A.; Grundlehner, J.; Mayr, M.; Kegel, M.; Schreier, G.; Hintermüller, C.; Hotter, M.; et al. Towards a Personal Health Record System for Mental Health: Implementation and Evaluation of the MyRecovery Hub System. *J. Med. Internet Res. Ment. Health* **2017**, *4*, e5.
6. World Health Organization. *Global Diffusion of eHealth: Making Universal Health Coverage Achievable*; World Health Organization: Geneva, Switzerland, 2016; Available online: https://apps.who.int/iris/bitstream/handle/10665/252529/9789241511780-eng.pdf?sequence=1 (accessed on 23 February 2023).
7. European Commission. *eHealth Action Plan 2012–2020: Innovative Healthcare for the 21st Century*; European Commission: Brussels, Belgium, 2012; Available online: https://ec.europa.eu/digital-single-market/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century (accessed on 23 February 2023).
8. Karacic, J. Europe, we Have a Problem! Challenges to Health Data-Sharing in the EU. In Proceedings of the 18th International Conference on Wireless and Mobile Computing, Networking and Communications [WiMob], Thessaloniki, Greece, 10–12 October 2022; pp. 47–50.
9. Gomes, R.M.; Pinheiro, P.; Ferreira, D.; Moreira, F.; Coimbra, M.; Rodrigues, P.P.; Silva, A.; Simões, R.; Alves, V.; Santos, M.Y.; et al. Ethics in Digital Health. *J. Med. Syst.* **2021**, *45*, 80.
10. Nunes, R. *Healthcare as a Universal Human Right: Sustainability in Global Health*; Routledge: London, UK; New York, NY, USA, 2022.
11. Correia, M.; Rego, G.; Nunes, R. Gender transition: Is there a right to be forgotten. *Health Care Anal.* **2021**, *29*, 283–300. [CrossRef] [PubMed]
12. Torous, J.; Roberts, L.W.; Holtzheimer, P.E. (Eds.) *Ethical and Legal Issues in Digital Health*; Academic Press: Cambridge, MA, USA, 2019.
13. American Medical Association. Patient Rights. Available online: https://www.ama-assn.org/delivering-care/ethics/patient-rights (accessed on 25 February 2023).
14. Pritts, J.L. The importance and value of protecting the privacy of health information: Roles of the HIPAA Privacy Rule and the Common Rule in health research. *Mich. State Law Rev.* **2006**, *2006*, 1307–1329.
15. Gurvich, A. *The Right to Privacy in the Digital Age*; The New York Times: New York, NY, USA, 2013; Available online: https://www.nytimes.com/roomfordebate/2013/11/22/the-right-to-privacy-in-the-digital-age (accessed on 23 February 2023).
16. Robillard, J.M.; Johnson, T.W.; Hennessey, C.; Beattie, B.L.; Illes, J.; Juengst, E.T.; Keay-Bright, W.; Lidster, R.T.; Rouleau, G.; Smith, M.J. *Engaging Privacy and Information Technology in a Digital Age*; National Academies Press: Washington, DC, USA, 2016. Available online: https://www.ncbi.nlm.nih.gov/books/NBK424347/ (accessed on 23 February 2023).
17. Sweeney, L. Privacy: A precious right and a fundamental freedom. *J. Law Med. Ethics* **2009**, *37*, 712–722.
18. Li, Y.; Li, L. Privacy protection for patient data sharing in clinical trials. *BMC Med. Ethics* **2019**, *20*, 56.
19. Schwartz, A.H.; Kulikowski, C.A. Data protection and privacy issues for healthcare information technology. *J. Am. Med. Inform. Assoc.* **2008**, *15*, 283–292.
20. Kierkegaard, P. Health data exchange and data protection across borders: The example of the EU and the USA. *Int. J. Med. Inform.* **2007**, *76*, 133–141.
21. European Union. General Data Protection Regulation. Regulation [EU] 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data. 2016. Available online: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679 (accessed on 23 February 2023).
22. European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*; European Commission: Brussels, Belgium, 2022.
23. Eysenbach, G. What is e-health? *J. Med. Internet Res.* **2001**, *3*, e20. [CrossRef] [PubMed]
24. Oh, H.; Rizo, C.; Enkin, M.; Jadad, A. What is eHealth (3): A systematic review of published definitions. *J. Med. Internet Res.* **2005**, *7*, e1. [CrossRef] [PubMed]
25. Van den Berg, N.; Schumann, M.; Kraft, K.; Hoffmann, W.; Bender, M. Mobile health in oncology: A patient survey about app-assisted cancer care. *JMIR Mhealth Uhealth* **2012**, *1*, e11. [CrossRef]

26. Beigi, M.; Feizi Derakhshi, M.R.; Safdari, R. Patient privacy and security in the era of e-Health: Ethical considerations. *Acta Inform. Med.* **2016**, *24*, 168–172.
27. Varkey, B. Principles of Clinical Ethics and Their Application to Practice. *Med. Princ. Pract.* **2021**, *30*, 17–28. [CrossRef] [PubMed]

**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.