information

MDPI

Review

Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review

Ahmed Arafa [1,2,*], Haytham A. Sheerah [3] and Shada Alsalamah [4,5]

[1] Department of Preventive Cardiology, National Cerebral and Cardiovascular Center, Suita 564-8565, Japan
[2] Department of Public Health and Community Medicine, Faculty of Medicine, Beni-Suef University, Beni-Suef 62521, Egypt
[3] International Collaborations, Ministry of Health, Riyadh 11176, Saudi Arabia; hasheerah@moh.gov.sa
[4] Information Systems Department, College of Computer and Information Sciences, King Saud University, Riyadh 11362, Saudi Arabia; saalsalamah@ksu.edu.sa
[5] Digital Health and Innovation Department, World Health Organization, CH-1211 Geneva, Switzerland
* Correspondence: ahmed011172@med.bsu.edu.eg; Tel.: +81-6-6170-1070 (ext. 60239); Fax: +81-6-6170-1824

Abstract: Emerging digital technologies, such as telemedicine, artificial intelligence, the Internet of Medical Things, blockchain, and visual and augmented reality, have revolutionized the delivery of and access to healthcare services. Such technologies allow for real-time health monitoring, disease diagnosis, chronic disease management, outbreak surveillance, and rehabilitation. They help personalize treatment plans, identify trends, contribute to drug development, and enhance public health management. While emerging digital technologies have numerous benefits, they may also introduce new risks and vulnerabilities that can compromise the confidentiality, integrity, and availability of sensitive healthcare information. This review article discussed, in brief, the key emerging digital technologies in the health sector and the unique threats introduced by these technologies. We also highlighted the risks relevant to digital health cybersecurity, such as data breaches, medical device vulnerabilities, phishing, insider and third-party risks, and ransomware attacks. We suggest that the cybersecurity framework should include developing a comprehensive cybersecurity strategy, conducting regular risk assessments, implementing strong access control, encrypting data, educating staff, implementing secure network segmentation, backing up data regularly, monitoring and detecting anomalies, establishing an incident response plan, sharing threat intelligence, and auditing third-party vendors.

Keywords: artificial intelligence; blockchain; cybersecurity; digital health; emerging digital technologies; healthcare; telehealth

Citation: Arafa, A.; Sheerah, H.A.; Alsalamah, S. Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review. *Information* **2023**, *14*, 640. https://doi.org/10.3390/info14120640

Academic Editors: Jose de Vasconcelos, Hugo Barbosa and Carla Cordeiro

Received: 19 October 2023
Revised: 8 November 2023
Accepted: 28 November 2023
Published: 29 November 2023

1. Introduction

The healthcare industry has witnessed a profound transformation fueled by rapid advancements in digital technologies. Over the past few decades, emerging digital technologies have surfaced as powerful catalysts for innovation in healthcare. Telemedicine, wearable devices, electronic health records, the Internet of Things (IoT) in healthcare, artificial intelligence (AI), and blockchain technology are just a few examples of the technologies that have rapidly transformed the sector. Telemedicine has made healthcare more accessible by enabling remote consultations, wearable devices have allowed for continuous patient monitoring, electronic health records have streamlined record-keeping and data sharing, and AI has offered remarkable insights for diagnosis and treatment. The utilization of these technologies has improved healthcare efficiency and effectiveness, but it has also introduced new challenges [1–3].

The integration of digital technologies in healthcare has opened up Pandora's box of vulnerabilities. Interconnected devices, often with inadequate security measures, can be a point of entry for cyberattacks. Patient data, a prime target for hackers, are at risk

of theft or unauthorized access. The rapid pace of innovation sometimes means that security considerations are an afterthought, leaving systems and devices unprepared to face evolving threats. Moreover, the human element, including healthcare staff and patients, can also inadvertently introduce vulnerabilities through actions such as sharing passwords, falling victim to phishing attacks or failing to update software and systems regularly. As such, the vulnerabilities related to emerging digital technologies in healthcare demand a vigilant and proactive response [4–6].

Specifically, cybersecurity threats in healthcare have been on the rise, posing significant risks to patient safety and data integrity. Malware attacks, ransomware incidents, and data breaches have the potential to disrupt healthcare services, compromise patient records, and jeopardize the trust between healthcare providers and their patients. The consequences of these threats extend beyond financial losses, with the potential for harm to patient health and wellbeing. Moreover, healthcare institutions also face legal and reputational repercussions, making cybersecurity a paramount concern. Understanding these threats and their potential impacts is crucial in the ongoing effort to safeguard the healthcare industry from malicious actions [5–7].

In response to the growing threats, healthcare organizations have been actively developing and implementing cybersecurity best practices. The approach includes ensuring robust security measures across digital healthcare systems, securing endpoints and networks, encrypting sensitive data, and training personnel to recognize and mitigate cyber risks. Furthermore, regulatory frameworks and standards mandate certain cybersecurity measures to protect patient data. Collaboration among healthcare stakeholders, governments, and the cybersecurity industry has also been instrumental in developing effective strategies to bolster the security of emerging digital technologies in healthcare [5–7].

In this context, the World Health Organization's (WHO) Global Strategy on Digital Health 2020–2025 highlighted the need for harnessing the power of digital technologies alongside strengthening data protection and privacy measures in digital health systems. These strategic objectives underscore the importance of establishing robust legal and regulatory frameworks to safeguard the privacy, confidentiality, and integrity of personal health data [8].

In an era where technology has the potential to revolutionize healthcare, it is crucial to strike a balance between harnessing the power of these digital advancements and ensuring that they do not become vectors of harm. In doing so, we can pave the way for a future where emerging digital technologies in healthcare can be harnessed to their full potential, delivering optimal patient care while safeguarding patient data and well-being from the ever-present cybersecurity threats.

Unlike previous review articles that discussed certain technical areas related to emerging digital technologies, this review article will navigate through interconnected facets of emerging digital technologies in healthcare and cybersecurity, aiming to provide a comprehensive understanding of the current landscape, especially for healthcare workers. By exploring the benefits, vulnerabilities, threats, and best practices in healthcare cybersecurity, readers will gain insights into the intricate dance between innovation and security within the healthcare sector.

2. Methods

The primary objective of this narrative review is to provide a comprehensive and insightful overview of emerging digital technologies in healthcare, with a particular focus on cybersecurity considerations. We aim to synthesize the existing literature to understand the current landscape of digital technologies in healthcare and the challenges and opportunities related to cybersecurity within this context (Table 1).

Table 1. A summary of items discussed in this narrative review.

Emerging Digital Technologies in Healthcare	Vulnerabilities Related to Emerging Digital Technologies in Healthcare	Cybersecurity Threats in Healthcare	Cybersecurity Best Practices in the Health Sector
• Mobile health applications (mHealth apps), wearable Internet of Things (WIoT), and personalized health (pHealth)	• Cybersecurity	• Data breaches	• Develop a comprehensive cybersecurity strategy
• Big data analytics	• Interoperability	• Medical device vulnerabilities	• Conduct regular risk assessments
• Cloud computing	• Regulatory compliance	• Phishing	• Implement strong access controls
• Internet of Medical Things (IoMT)	• Ethical considerations	• Insider risks	• Encrypt data
• Virtual reality (VR) and augmented reality (AR)	• Provider and patient education	• Third-party risks	• Educate and train staff
• Telemedicine and telehealth	• Infrastructure	• Ransomware attacks	• Implement secure network segmentation
• Artificial intelligence (AI) and machine learning (ML)			• Regularly back up data
• Distributed Ledger Technology (DLT) and blockchain			• Monitor and detect anomalies
			• Establish an incident response plan
			• Collaborate and share threat intelligence
			• Regularly audit and assess third-party vendors

We accessed a variety of academic databases, including, but not limited to, PubMed and Scopus. We employed a combination of keywords and phrases, including "digital technologies in healthcare", "eHealth", "mHealth", "telemedicine", "cybersecurity", "healthcare data security", "emerging technologies in healthcare", and related terms. These keywords were used in various combinations to maximize the relevance of the search results. Non-peer-reviewed studies and studies published in languages other than English were not sought.

The results and insights extracted from the selected literature were synthesized in a narrative format. This narrative review does not include a meta-analysis but instead provides a qualitative analysis of the themes, trends, and issues related to the adoption of digital technologies in healthcare and the challenges posed by cybersecurity. Due to the multi-faceted nature of our topic, the need to cover several aspects related to emerging digital technologies in healthcare and threats related to their application, and the large number of articles investigating specific areas, we could not systematically obtain all related articles, and we focused on narrative and systematic reviews instead. We believe that a narrative review may allow healthcare workers to obtain a more comprehensive view of emerging digital technologies in healthcare and cybersecurity. Nevertheless, it is important to acknowledge that this narrative review may be subject to certain limitations. The inclusion criteria may introduce selection bias, and the rapidly evolving nature of the field might mean that some emerging developments may not be adequately covered.

3. Emerging Digital Technologies in Healthcare

There are several emerging digital technologies that are making an impact on healthcare. These technologies use digital platforms, connectivity, and data to transform various aspects of healthcare delivery, patient engagement, and research. Regardless of the technology, they all mainly aim to connect health workers and patients to enable a seamless flow of medical information between healthcare settings for informed decision-making purposes [8] (Table 2).

Table 2. A summary of the main features of emerging digital technologies in healthcare.

Features	Summary
Types and uses of mobile health applications (mHealth apps)	Health tracking, medication, telemedicine and telehealth, fitness, mental health, health record, and health education
Features of wearable Internet of Things (WIoT)	Wireless mobility, intelligence and interactivity, sustainability, simple operation, and portability
Types of big data streams	Clinical data from electronic medical records, biometric data from medical devices, financial data from relevant financial records, patient data from questionnaires and surveys, and social media data from social network
Implications of cloud computing	Relying on software, providing security and interoperability, performing clinical tasks, supporting patient-centeredness, facilitating collaboration, and increasing service mobility and flexibility
Steps of the Internet of Medical Things (IoMT)	Collecting and analyzing data, informing healthcare providers, patients, or other medical devices, and sending real-time recommendations
Uses of virtual reality (VR) and augmented reality (AR)	Medical training, surgical planning, remote consultations, and patient education
Challenges to virtual reality (VR) and augmented reality (AR)	High cost, difficulty in integrating VR and AR with existing healthcare infrastructure, and ethical and legal considerations
Types of telemedicine	Remote patient monitoring, store-and-forward telemedicine, real-time telemedicine, and physician-to-physician consultation
Uses of artificial intelligence (AI) and machine learning (ML)	Analyzing medical data, developing personalized treatment plans, remotely tracking patient vital signs, symptoms, and adherence to treatment plans, and automating routine administrative tasks, such as appointment scheduling, documentation, and data entry
Applications of blockchain technology	Health data exchange, medical supply chain management, clinical trials and research, health insurance and claims processing, and personal health records

3.1. Mobile Health Applications (mHealth Apps), Wearable Internet of Things (WIoT), and Personalized Health (pHealth)

mHealth apps are applications designed for mobile devices, such as smartphones and tablets, that aim to support healthcare delivery and promote wellness. They vary widely in terms of content, accessibility, interactivity, connectivity, and security [9]. They offer a wide range of functionalities and can be categorized into the following several types, based on their uses: (1) health tracking apps, which focus on monitoring and tracking health-related data, such as physical activity, sleep patterns, nutrition, and vital signs; (2) medication apps, which send reminders for medication doses, track adherence, provide information about drug interactions, and enable users to maintain a medication schedule; (3) telemedicine and telehealth apps, which enable patients to connect with healthcare providers through video calls, text messaging, or voice calls, allowing for remote diagnosis, monitoring, and treatment; (4) fitness apps, which offer workout tracking, personalized training plans, and

step counting; (5) mental health apps, which provide resources for mental health support, stress management, and mindfulness practices; (6) health record apps, which enable users to store, access, and manage their personal health information and keep track of their medical history, test results, vaccinations, and appointments; and (7) health education apps, which provide health-related education, information, and resources [9–12].

WIoT interconnects wearable sensors to enable the monitoring of human factors and other data, which is useful in enhancing individuals' everyday quality of life. The main features of WIoT are as follows: (1) wireless mobility, (2) intelligence and interactivity, (3) sustainability, (4) simple operation, and (5) portability [10]. They can be categorized, per their applications, into four areas: (1) health monitoring, (2) disease diagnosis, (3) chronic disease management, and (4) rehabilitation [10].

pHealth refers to the use of digital health technologies, data analytics, and personalized medicine approaches to tailor healthcare and preventive interventions to patients' characteristics, needs, and preferences. The concept of pHealth aims to move away from the traditional "one-size-fits-all" approach to healthcare and move toward more personalized and patient-centered care. pHealth uses various technologies, such as WIoT, mHealth apps, genetic testing, and remote monitoring tools, to collect and analyze vast amounts of data about an individual's health status, behaviors, and lifestyle factors. By combining these data with advanced analytics, healthcare providers can gain deeper insights into a person's health profile and make more informed and targeted health decisions [13].

However, several challenges face the wide application of mHealth apps and WIoT, such as the lack of industry standards, obstacles in reaching user-friendly solutions, cybersecurity concerns, and technical problems [9–12].

3.2. Big Data Analytics

Big data streams include various types of data: (1) clinical data from electronic medical records, hospital information systems, image centers, laboratories, and pharmacies; (2) biometric data from medical devices that monitor vital signs, body composition, etc.; (3) financial data, constituting records of relevant financial operations; (4) scientific research data; (5) patient data, including treatment preferences, satisfaction levels, self-administered information about their lifestyle and sociodemographic factors; and (6) social media data [14]. Big data analytics involves processing and analyzing a huge amount of data. This processing may vary in terms of data volume, speed of generation, heterogeneity, inconsistency, quality, and value [14]. Big data analytics has become increasingly used to improve clinical decision-making, identify trends, contribute to drug development, and enhance public health management [14–17]. However, big data analytics faces several challenges related to storage, processing, finding and fixing troubles, and security issues [16,17].

3.3. Cloud Computing

Cloud computing offers scalable and cost-effective storage and processing capabilities for healthcare organizations. It enables secure access to medical records, facilitates data sharing and collaboration, and supports telemedicine and remote monitoring [18–21]. The implications of cloud computing in healthcare can be summarized in the following points: (1) relying on software, especially software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS); (2) providing security and interoperability; (3) performing clinical tasks; (4) supporting patient-centeredness; (5) facilitating collaboration; and (6) increasing service mobility and flexibility [19]. However, the lack of regulations, system outages, lack of control, and security issues remain potential challenges [19–21] (Figure 1).

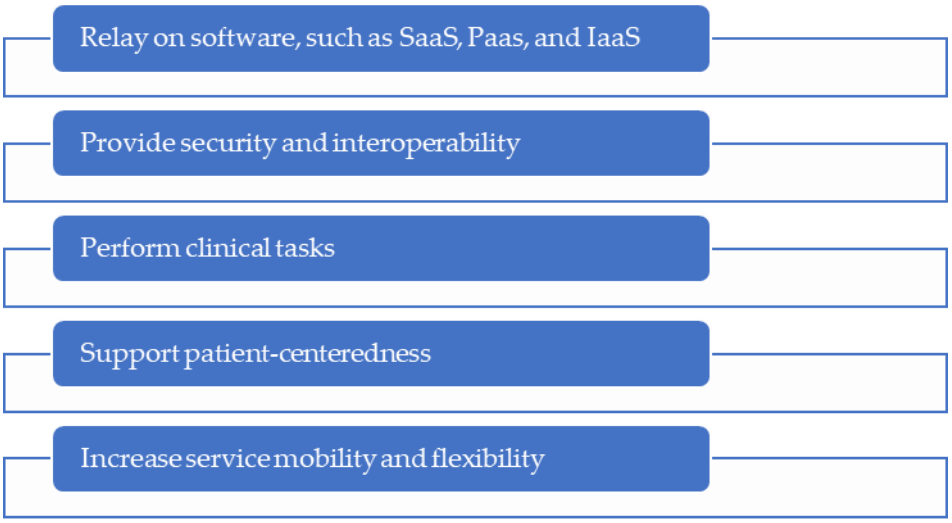

Figure 1. Characteristics of cloud computing as an emerging digital technology in healthcare.

3.4. Internet of Medical Things (IoMT)

The IoMT refers to the interconnected network of medical devices, sensors, and wearable technologies, such as smartwatches, fitness trackers, and glucose monitors. These devices collect and transmit instantaneous health data, allowing for remote patient monitoring, early disease detection, and personalized care [22–24]. The IoMT framework-based digital healthcare includes several stages. First, the patient's data are collected using smart wearable or implanted devices that are connected by a body or wireless sensor network, then analyzed, and finally, predictions are drawn. Healthcare providers, patients, or other medical devices can be automatically approached to be informed of the current medical condition or future potential health outcome. Finally, the IoMT provides real-time recommendations about what should be conducted to manage the current medical condition and prevent future complications [22]. Nevertheless, the IoMT faces challenges related to data privacy, a potential lack of accuracy, especially when massive data are processed, and the high cost of installing and maintaining the devices [22–24].

3.5. Virtual Reality (VR) and Augmented Reality (AR)

VR and AR technologies create interactive experiences for medical training, surgical planning, and patient education. While VR can simulate realistic medical scenarios for training healthcare professionals, AR overlays digital information in the real world, aiding in surgical navigation and medical imaging [25–28]. In medical training, VR and AR technologies provide interactive environments for medical students, allowing them to simulate surgeries, practice complex procedures, and learn anatomy in a realistic and risk-free manner. These technologies enable hands-on experiences and improve learning outcomes. Surgeons can use VR and AR to visualize patient-specific anatomical structures and plan complex surgeries. VR can be used in rehabilitation to create engaging and motivating environments for patients. It can be used to simulate real-life scenarios and exercises, helping patients to regain motor skills, improve balance, and manage pain. AR can provide feedback and guidance during physical therapy sessions. Furthermore, VR and AR can facilitate remote consultations by providing virtual meeting spaces where healthcare providers can interact with patients and review medical data. It allows for better collaboration, faster diagnoses, and reduced travel burdens for patients [25–28]. The main challenge of VR and AR is the high cost of high-quality headsets, sensors, and computing systems. Moreover, integrating VR and AR systems with existing healthcare infrastructure, electronic health records, and medical imaging systems can be complex. Furthermore, the use of VR and AR in healthcare raises ethical and legal considerations related to patient privacy, data security, and informed consent [25–28].

3.6. Telemedicine and Telehealth

Telemedicine refers to the remote delivery of healthcare services, including medical consultations, diagnoses, and treatment, using telecommunications technology. The main types of telemedicine are remote patient monitoring, store-and-forward telemedicine, real-time interactive telemedicine, and physician-to-physician consultation [29–32]. It poses several advantages, such as providing convenient access to healthcare, especially for those in remote areas, eliminating travel expenses and time off work for patients, and reducing hospital admissions. However, many barriers should be considered, such as technological difficulties, particularly in rural and low-income areas, privacy and security concerns, limited physical examination, reimbursement and regulatory problems, and diagnostic limitations [29–32].

Telehealth is a broader term that encompasses a wider range of healthcare services and activities beyond merely clinical care. It includes the use of digital communication technologies to provide healthcare-related information, education, and administrative services. It can involve remote patient monitoring, health education through online platforms, electronic health record systems, mobile health apps, and administrative tasks such as scheduling appointments and processing medical bills [29–32] (Figure 2).

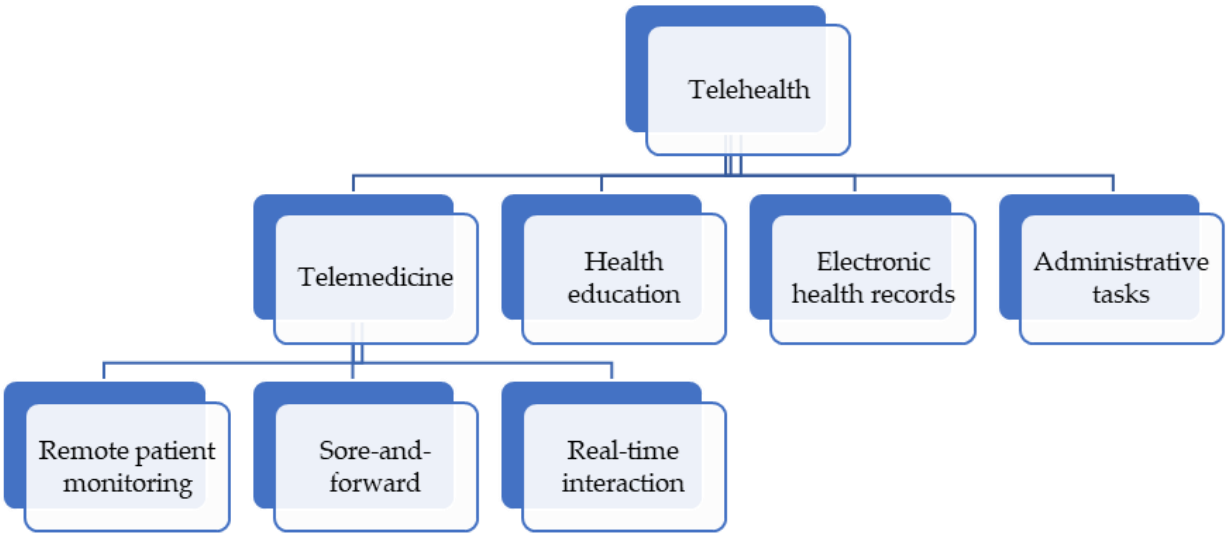

Figure 2. Telehealth as an emerging digital technology in healthcare.

3.7. Artificial Intelligence (AI) and Machine Learning (ML)

AI refers to the ability of machines to mimic human behavior by learning from data using self-learning technologies (such as data mining, pattern recognition, and natural language processing) to understand the way the human brain works. ML is a subset of AI that can also improve with experience. With such techniques, AI and ML have the potential to revolutionize healthcare. They can analyze vast amounts of medical data, including medical images, lab results, and patient records, to aid in the diagnosis of diseases. By analyzing individual patient data, AI and ML can develop personalized treatment plans based on factors, such as medical history, genetics, and lifestyle. AI-powered monitoring devices can remotely track patient vital signs, symptoms, and adherence to treatment plans. ML algorithms can detect trends and anomalies, alerting healthcare providers to potential issues. Furthermore, AI can automate routine administrative tasks, such as appointment scheduling, documentation, and data entry, allowing healthcare professionals to focus more on patient care [33–36]. However, data privacy concerns, a lack of quality data, inadequate interpretations, the lack of a skilled workforce, and regulatory and legal shortages are the main barriers to the wide application of AI and ML in medical facilities [37,38].

3.8. Distributed Ledger Technology (DLT) and Blockchain

DLT is a decentralized and distributed digital system that records transactions and data across multiple computers or nodes. In a distributed ledger, each participant has a copy of the data, and changes made to the ledger are synchronized across all copies. This approach ensures the transparency, security, and immutability of data, since alterations require consensus among the network participants. Blockchain is a specific type of DLT that uses cryptographic techniques to secure and validate transactions. It is a chain of blocks, where each block contains a list of transactions and a reference to the previous block, forming an unbroken and tamper-evident chain. The key features of blockchain include decentralization, immutability, and transparency. Blockchain technology has several potential applications, such as (1) health data exchange: blockchain can facilitate and secure interoperable exchange of patient health records among healthcare providers while maintaining data privacy and consent; (2) medical supply chain management: blockchain can track the movement of pharmaceuticals, medical devices, and supplies, ensuring authenticity, quality control, and reducing the risk of counterfeit products; (3) clinical trials and research: blockchain can enhance transparency and data integrity in clinical trials, helping to prevent data manipulation and improving the research process; (4) health insurance and claims processing: blockchain can streamline insurance processes, reduce fraud, and improve the accuracy and speed of claims processing; and (5) personal health records: blockchain can enable patients to have more control over their health data, allowing them to share specific information with healthcare providers and researchers while maintaining ownership and privacy (Figure 3). Implementing blockchain in healthcare requires addressing challenges such as regulatory compliance, data standardization, scalability, and ensuring that private patient data remains secure [39–43].

Figure 3. Applications of blockchain as an emerging digital technology in healthcare.

4. Vulnerabilities Related to Emerging Digital Technologies in Healthcare

While emerging digital technologies have numerous benefits, they also introduce new threats and vulnerabilities that can compromise the confidentiality, integrity, and availability of sensitive healthcare information.

4.1. Cybersecurity

The increased use of digital technologies in healthcare generates and collects vast amounts of sensitive patient data. Ensuring robust data security and privacy measures is crucial to protect against data breaches, unauthorized access, and the potential misuse of personal health information. Medical facilities should implement strong encryption, access controls, and data anonymization techniques to safeguard patient data [44–51]; this topic is described below with more details.

4.2. Interoperability

Interoperability refers to the ability of different digital systems and technologies to exchange and use data seamlessly. Interoperability challenges could be due to the following. (1) A lack of standardization: The absence of widely adopted standards for data formats, interfaces, and communication makes it difficult for systems to exchange and interpret data accurately. (2) Fragmented systems and technical heterogeneity: Healthcare organizations often use multiple digital systems, such as electronic health records, imaging systems, laboratory systems, and telemedicine platforms. Bridging the gaps between these systems to enable data exchange is a significant challenge. (3) Data security: Healthcare data are highly sensitive and subject to strict privacy regulations. Ensuring secure and private data exchange between digital systems while complying with security regulations adds complexity to achieving interoperability. (4) Inadequate infrastructure: Several medical facilities may use outdated technologies with limited data exchange capabilities. Integrating newer digital technologies with older systems is challenging. Addressing these challenges requires collaborative efforts among stakeholders, including healthcare organizations, technology vendors, standardization bodies, and regulatory agencies [52–54].

4.3. Regulatory Compliance

Healthcare is an industry with numerous legal and regulatory requirements. Compliance with these regulations becomes more complex with the adoption of digital technologies, especially in multiple jurisdictional settings. Medical facilities should navigate the regulatory landscape and ensure that their digital systems adhere to the necessary privacy and security standards [55–57]. Several regulatory bodies pertain to digital health technologies. In the US, for example, the Health Insurance Portability and Accountability Act (HIPAA) has established standards for the protection of patient health information, while the Food and Drug Administration (FDA) regulates medical devices, including certain digital health technologies, such as software applications, wearables, and telehealth devices [56]. In the European Union, the General Data Protection Regulation (GDPR) has applied rules for the protection of personal data, while the Medical Device Regulation (MDR) regulates medical devices, including those related to digital health [55]. Nevertheless, these regulations struggle to keep pace with the rapid advancements in digital healthcare. Furthermore, several digital technologies fall into gray regulatory areas, such as guidelines and frameworks. In addition, regulatory bodies face challenges in monitoring evolving digital technologies, detecting non-compliance, and enforcing regulations effectively [56].

4.4. Ethical Considerations

The use of emerging digital technologies in healthcare raises ethical questions related to data ownership, consent, transparency, and bias. The main ethical considerations can be summarized in the following points: (1) data privacy and security: digital technologies generate vast amounts of sensitive patient data, raising concerns about privacy breaches and data security; (2) informed consent issues: patients should be adequately informed about the potential risks, benefits, and possible uses of their data, enabling them to make informed decisions about their participation in digital health initiatives; (3) algorithm bias: AI and machine learning algorithms can inadvertently introduce bias, leading to unequal treatment and disparities in healthcare outcomes; (4) patient autonomy: patients should have the ability to make choices about the use, sharing, and retention of their health information; (5) access and equity: technological literacy, socioeconomic disparities, and geographical location can create barriers to access; (6) transparency: AI and machine learning algorithms can be complex and difficult to understand, making it challenging to explain their decisions or actions; and (7) accountability: establishing clear lines of accountability and defining liability frameworks becomes essential to protect both patients and healthcare providers [58–60].

4.5. Provider and Patient Education

The successful adoption and utilization of emerging digital technologies require adequate education and training for healthcare providers and patients. Healthcare providers should be proficient in using these technologies effectively, while patients need to be educated about the benefits, risks, and privacy considerations related to the use of digital tools [61–63].

4.6. Infrastructure

The infrastructure required to support emerging digital technologies may be lacking in certain regions or medical facilities. The main components of the infrastructure needed for installing digital technologies in medical facilities are the following: (1) a reliable and high-speed network to provide seamless connectivity and data transmission, (2) hardware and devices, (3) an electronic health recording system, and (4) technical support and maintenance [64,65].

5. Cybersecurity Threats in Healthcare

Insufficient cybersecurity regulations and procedures in medical facilities pose significant threats to patient safety, data integrity, and healthcare management. The healthcare sector has become an attractive target for cybercriminals due to the high value of medical records.

5.1. Data Breaches

Breached data can include medical records, personal identifiers, financial data, and insurance details. The stolen data can be sold to advertising agencies or used for identity theft or financial fraud, leading to significant harm to individuals and reputational damage to medical facilities [66,67].

5.2. Medical Device Vulnerabilities

The increasing use of interconnected medical devices, such as infusion pumps, pacemakers, and imaging systems, introduces vulnerabilities. These devices may have outdated software or weak security controls, making them susceptible to cyberattacks [68,69].

5.3. Phishing

Phishing attacks target healthcare employees through deceptive emails, phone calls, or text messages. These attacks could trick individuals into revealing sensitive information or granting unauthorized access, leading to data breaches [70–72].

5.4. Insider Risks

Insiders, including employees, contractors, or partners, pose a significant cybersecurity risk. Insider threats can involve intentional actions, such as stealing or leaking data, or unintentional actions, such as inadvertently exposing sensitive information [73–76].

5.5. Third-Party Risks

Medical facilities often collaborate with third-party vendors, suppliers, and partners, increasing the attack surface. Weak security practices in these third-party systems can be exploited by cybercriminals to obtain unauthorized access to healthcare networks [75,76].

5.6. Ransomware Attacks

Ransomware has emerged as a major threat to medical facilities. These attacks involve malicious software that encrypts data, rendering it inaccessible until a ransom is paid. Ransomware can lead to significant disruptions in healthcare services, compromise patient care, and result in financial losses [77,78].

6. Cybersecurity Best Practices in the Health Sector: A Framework for Healthcare Settings

6.1. Develop a Comprehensive Cybersecurity Strategy

Medical facilities should establish a robust cybersecurity strategy that outlines clear objectives, policies, and procedures for protecting patient data and critical infrastructure. This strategy should encompass prevention, detection, response, and recovery mechanisms to address potential cyber threats effectively [45,46,79,80].

6.2. Conduct Regular Risk Assessments

Regular risk assessments help identify vulnerabilities and potential entry points for cyberattacks. By assessing the security posture of systems, networks, and devices, healthcare organizations can proactively identify and mitigate potential risks and weaknesses [79,80].

6.3. Implement Strong Access Controls

Strong access controls are essential to prevent unauthorized access to sensitive patient data. Implementing multi-factor authentication, strong passwords, and role-based access control ensures that only authorized individuals can access critical information [80].

6.4. Encrypt Data

Encryption is a fundamental measure for protecting patient data. It ensures that even if data were to be intercepted or stolen, they remain unreadable and unusable. Encryption should be applied to data at rest, in transit, and during backup processes [81,82].

6.5. Educate and Train Staff

Human error remains a significant factor in cybersecurity incidents. Medical facilities should conduct regular training and awareness programs to educate employees about cybersecurity risks, best practices, and the importance of following security protocols [83]. This education can take various forms, including lectures, seminars, and even games [84–86].

6.6. Implement Secure Network Segmentation

The segmentation of networks and systems within healthcare environments helps contain potential breaches and limit the lateral movement of attackers. By separating different areas of the network and implementing strict access controls between them, medical facilities can reduce the impact of a successful cyberattack [87].

6.7. Regularly Back up Data

Backing up data is crucial to ensure continuity and recovery from potential ransomware attacks or data loss incidents. Backups should be encrypted, stored securely, and tested regularly to verify their integrity and the ability to restore data effectively [88,89].

6.8. Monitor and Detect Anomalies

Implementing robust monitoring and detection systems can help identify and respond to cybersecurity incidents promptly. Intrusion detection and prevention systems, security information and event management tools, and immediate log analysis can aid in detecting and mitigating threats promptly [80].

6.9. Establish an Incident Response Plan

Medical facilities should have a well-defined incident response plan in place. This plan outlines the steps to be taken in the event of a cybersecurity incident, including communication protocols, containment measures, forensic investigation procedures, and recovery strategies [80].

6.10. Collaborate and Share Threat Intelligence

Medical facilities should actively participate in information sharing and collaborate with industry peers, government agencies, and cybersecurity organizations to stay updated

on emerging threats, vulnerabilities, and best practices. Sharing threat intelligence enhances the collective ability to defend against cyber threats [90].

6.11. Regularly Audit and Assess Third-Party Vendors

Medical facilities often work with third-party vendors who have access to patient data or provide critical services. It is essential to assess the security practices of these vendors and ensure they meet stringent cybersecurity standards.

7. Conclusions

Emerging digital technologies are transforming the landscape of healthcare, ushering in an era of innovation and efficiency. These technologies, including mHealth apps, wearables, big data analytics, cloud computing, blockchain, IoMT, VR, AR, telemedicine, AI, and ML, are instrumental in revolutionizing healthcare services. mHealth apps and wearables empower individuals to monitor their health in real time, fostering proactive healthcare management. Big data analytics enable healthcare professionals to extract valuable insights from vast datasets, personalizing treatment plans and identifying disease trends for public health benefit. Cloud computing facilitates seamless data sharing and storage, enhancing collaboration and accessibility. Blockchain technology ensures the integrity and security of medical records, assuaging concerns about data privacy and accuracy. IoMT devices connect healthcare systems, enhancing patient care coordination and remote monitoring. VR and AR technologies have applications in medical training and patient engagement, while telemedicine and telehealth platforms bridge geographical gaps, providing access to medical expertise and services. AI and ML algorithms aid in diagnosis and treatment, revolutionizing healthcare delivery. However, these transformative technologies also confront several challenges, such as cybersecurity threats, interoperability issues, regulatory complexities, ethical dilemmas, and the need for comprehensive provider and patient education. Infrastructure limitations further impede their widespread adoption. To mitigate cybersecurity risks, a robust framework is essential. This framework includes developing a comprehensive cybersecurity strategy, conducting regular risk assessments, enforcing strict access controls, data encryption, staff education, secure network segmentation, routine data backups, anomaly detection, incident response planning, threat intelligence sharing, and third-party vendor audits. By addressing these challenges, healthcare can harness the full potential of these digital innovations to improve patient care and public health outcomes.

Author Contributions: Conceptualization, A.A. and S.A.; methodology, A.A.; software, A.A.; validation, A.A., H.A.S. and S.A.; formal analysis, A.A.; investigation, A.A.; resources, A.A., H.A.S. and S.A.; data curation, A.A.; writing—original draft preparation, A.A.; writing—review and editing, A.A., H.A.S. and S.A.; visualization, A.A., H.A.S. and S.A.; supervision, A.A.; project administration, A.A.; funding acquisition, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data was created.

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

References

1. Stern, A.D.; Brönneke, J.; Debatin, J.F.; Hagen, J.; Matthies, H.; Patel, S.; Clay, I.; Eskofier, B.; Herr, A.; Hoeller, K.; et al. Advancing digital health applications: Priorities for innovation in real-world evidence generation. *Lancet Digit. Health* **2022**, *4*, e200–e206. [CrossRef] [PubMed]
2. Ronquillo, Y.; Meyers, A.; Korvek, S.J. *Digital Health*; StatPearls Publishing: Treasure Island, FL, USA, 2023.
3. Stoumpos, A.I.; Kitsios, F.; Talias, M.A. Digital transformation in healthcare: Technology acceptance and its applications. *Int. J. Environ. Res. Public Health* **2023**, *20*, 3407. [CrossRef] [PubMed]
4. Neves, A.L.; Burgers, J. Digital technologies in primary care: Implications for patient care and future research. *Eur. J. Gen. Pract.* **2022**, *28*, 203–208. [CrossRef] [PubMed]
5. Giansanti, D. Ten years of telehealth and digital healthcare: Where are we? *Healthcare* **2023**, *11*, 875. [CrossRef] [PubMed]

6. Mesko, B. Health IT and digital health: The future of health technology is diverse. *J. Clin. Transl. Res.* **2018**, *3* (Suppl. S3), 431–434. [CrossRef] [PubMed]
7. Ibrahim, M.S.; Yusoff, H.M.; Abu Bakar, Y.I.; Aung, M.M.T.; Abas, M.I.; Ramli, R.A. Digital health for quality healthcare: A systematic mapping of review studies. *Digit. Health* **2022**, *8*, 20552076221085810. [CrossRef] [PubMed]
8. Mariano, B. Towards a global strategy on digital health. *Bull. World Health Organ.* **2020**, *98*, 231. [CrossRef] [PubMed]
9. Nouri, R.; RNiakan Kalhori, S.; Ghazisaeedi, M.; Marchand, G.; Yasini, M. Criteria for assessing the quality of mHealth apps: A systematic review. *J. Am. Med. Inform. Assoc.* **2018**, *25*, 1089–1098. [CrossRef]
10. Lu, L.; Zhang, J.; Xie, Y.; Gao, F.; Xu, S.; Wu, X.; Ye, Z. Wearable health devices in health care: Narrative systematic review. *JMIR Mhealth Uhealth* **2020**, *8*, e18907. [CrossRef]
11. Smuck, M.; Odonkor, C.A.; Wilt, J.K.; Schmidt, N.; Swiernik, M.A. The emerging clinical role of wearables: Factors for successful implementation in healthcare. *NPJ Digit. Med.* **2021**, *4*, 45. [CrossRef]
12. Canali, S.; Schiaffonati, V.; Aliverti, A. Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. *PLoS Digit Health* **2022**, *1*, e0000104. [CrossRef] [PubMed]
13. Alsalamah, H.A.; Nasser, S.; Alsalamah, S.; Almohana, A.I.; Alanazi, A.; Alrrshaid, F. Wholesome Coin: A pHealth solution to reduce high obesity rates in Gulf Cooperation Council countries using cryptocurrency. *Front. Blockchain* **2021**, *4*, 654539. [CrossRef]
14. Batko, K.; Ślęzak, A. The use of big data analytics in healthcare. *J. Big Data* **2022**, *9*, 3. [CrossRef] [PubMed]
15. Piovani, D.; Bonovas, S. Real world-big data analytics in healthcare. *Int. J. Environ. Res. Public Health* **2022**, *19*, 11677. [CrossRef] [PubMed]
16. Cozzoli, N.; Salvatore, F.P.; Faccilongo, N.; Milone, M. How can big data analytics be used for healthcare organization management? Literary framework and future research from a systematic review. *BMC Health Serv. Res.* **2022**, *22*, 809. [CrossRef] [PubMed]
17. Nascimento, I.J.B.D.; Marcolino, M.S.; Abdulazeem, H.M.; Weerasekara, I.; Azzopardi-Muscat, N.; Gonçalves, M.A.; Novillo-Ortiz, D. Impact of big data analytics on people's health: Overview of systematic reviews and recommendations for future studies. *J. Med. Internet Res.* **2021**, *23*, e27275. [CrossRef] [PubMed]
18. Mehrtak, M.; SeyedAlinaghi, S.; MohsseniPour, M.; Noori, T.; Karimi, A.; Shamsabadi, A.; Heydari, M.; Barzegary, A.; Mirzapour, P.; Soleymanzadeh, M.; et al. Security challenges and solutions using healthcare cloud computing. *J. Med. Life* **2021**, *14*, 448–461. [CrossRef]
19. Gao, F.; Thiebes, S.; Sunyaev, A. Rethinking the meaning of cloud computing for health care: A taxonomic perspective and future research directions. *J. Med. Internet Res.* **2018**, *20*, e10041. [CrossRef]
20. Gu, D.; Yang, X.; Deng, S.; Liang, C.; Wang, X.; Wu, J.; Guo, J. Tracking knowledge evolution in cloud health care research: Knowledge map and common word analysis. *J. Med. Internet Res.* **2020**, *22*, e15142. [CrossRef]
21. Cresswell, K.; Domínguez Hernández, A.; Williams, R.; Sheikh, A. Key challenges and opportunities for cloud technology in health care: Semistructured interview study. *JMIR Hum. Factors* **2022**, *9*, e31246. [CrossRef]
22. Srivastava, J.; Routray, S.; Ahmad, S.; Waris, M.M. Internet of Medical Things (IoMT)-based smart healthcare system: Trends and progress. *Comput. Intell. Neurosci.* **2022**, *2022*, 7218113. [CrossRef]
23. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral. Biol. Craniofac. Res.* **2022**, *12*, 302–318. [CrossRef]
24. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A.; Yelamarthi, K. Prospect of Internet of Medical Things: A review on security requirements and solutions. *Sensors* **2022**, *22*, 5517. [CrossRef]
25. Bhugaonkar, K.; Bhugaonkar, R.; Masne, N. The trend of metaverse and augmented & virtual reality extending to the healthcare system. *Cureus* **2022**, *14*, e29071.
26. Yeung, A.W.K.; Tosevska, A.; Klager, E.; Eibensteiner, F.; Laxar, D.; Stoyanov, J.; Glisic, M.; Zeiner, S.; Kulnik, S.T.; Crutzen, R.; et al. Virtual and augmented reality applications in medicine: Analysis of the scientific literature. *J. Med. Internet Res.* **2021**, *23*, e25499. [CrossRef]
27. Kassutto, S.M.; Baston, C.; Clancy, C. Virtual, augmented, and alternate reality in medical education: Socially distanced but fully immersed. *ATS Sch.* **2021**, *2*, 651–664. [CrossRef]
28. Syed Abdul, S.; Upadhyay, U.; Salcedo, D.; Lin, C.W. Virtual reality enhancing medical education and practice: Brief communication. *Digit. Health* **2022**, *8*, 20552076221143948. [CrossRef]
29. Gajarawala, S.N.; Pelkowski, J.N. Telehealth benefits and barriers. *J. Nurse Pract.* **2021**, *17*, 218–221. [CrossRef]
30. Kichloo, A.; Albosta, M.; Dettloff, K.; Wani, F.; El-Amir, Z.; Singh, J.; Aljadah, M.; Chakinala, R.C.; Kanugula, A.K.; Solanki, S.; et al. Telemedicine, the current COVID-19 pandemic and the future: A narrative review and perspectives moving forward in the USA. *Fam. Med. Community Health* **2020**, *8*, e000530. [CrossRef]
31. Al-Hazmi, A.M.; Sheerah, H.A.; Arafa, A. Perspectives on telemedicine during the era of COVID-19; what can Saudi Arabia do? *Int. J. Environ. Res. Public Health* **2021**, *18*, 10617. [CrossRef]
32. Ibrahim, A.E.; Magdy, M.; Khalaf, E.M.; Mostafa, A.; Arafa, A. Teledermatology in the time of COVID-19. *Int. J. Clin. Pract.* **2021**, *75*, e15000. [CrossRef]
33. Bajwa, J.; Munir, U.; Nori, A.; Williams, B. Artificial intelligence in healthcare: Transforming the practice of medicine. *Future Heal. J.* **2021**, *8*, e188–e194. [CrossRef]

34. Briganti, G.; Le Moine, O. Artificial intelligence in medicine: Today and tomorrow. *Front. Med.* **2020**, *7*, 27. [CrossRef]
35. Habehh, H.; Gohel, S. Machine learning in healthcare. *Curr. Genom.* **2021**, *22*, 291–300. [CrossRef]
36. Althenayan, A.S.; AlSalamah, S.A.; Aly, S.; Nouh, T.; Mirza, A.A. Detection and classification of COVID-19 by radiological imaging modalities using deep learning techniques: A literature review. *Appl. Sci.* **2022**, *12*, 10535. [CrossRef]
37. Pujari, S.; Reis, A.; Zhao, Y.; Alsalamah, S.; Serhan, F.; Reeder, J.C.; Labrique, A.B. Artificial intelligence for global health: Cautious optimism with safeguards. *Bull. World Health Organ.* **2023**, *101*, 364. [CrossRef]
38. Oala, L.; Murchison, A.G.; Balachandran, P.; Choudhary, S.; Fehr, J.; Leite, A.W.; Goldschmidt, P.G.; Johner, C.; Schörverth, E.D.M.; Nakasi, R.; et al. Machine learning for health: Algorithm auditing & quality control. *J. Med. Syst.* **2021**, *45*, 105.
39. Alsalamah, H.A.; Alsuwailem, G.; Bin Rajeh, F.; Alharbi, S.; AlQahtani, S.; AlArifi, R.; AlShargi, S.; Alsalamah, S.A.; Alsalamah, S. eHomeCaregiving: A diabetes patient-centered blockchain ecosystem for COVID-19 caregiving. *Front. Blockchain* **2021**, *4*, 477012. [CrossRef]
40. Alsalamah, S.; Alsalamah, H.A.; Nouh, T.; Alsalamah, S.A. Healthyblockchain for global patients. *Comput. Mater. Contin.* **2021**, *68*, 2431–2449. [CrossRef]
41. Kurdi, H.; Alsalamah, S.; Alatawi, A.; Alfaraj, S.; Altoaimy, L.; Ahmed, S.H. HealthyBroker: A trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services. *Electronics* **2019**, *8*, 602. [CrossRef]
42. Saeed, H.; Malik, H.; Bashir, U.; Ahmad, A.; Riaz, S.; Ilyas, M.; Bukhari, W.A.; Khan, M.I.A. Blockchain technology in healthcare: A systematic review. *PLoS ONE* **2022**, *17*, e0266462. [CrossRef]
43. Elangovan, D.; Long, C.S.; Bakrin, F.S.; Tan, C.S.; Goh, K.W.; Yeoh, S.F.; Loy, M.J.; Hussain, Z.; Lee, K.S.; Idris, A.C.; et al. The use of blockchain technology in the health care sector: Systematic review. *JMIR Med. Inform.* **2022**, *10*, e17278. [CrossRef]
44. Jalali, M.S.; Kaiser, J.P. Cybersecurity in hospitals: A systematic, organizational perspective. *J. Med. Internet Res.* **2018**, *20*, e10059. [CrossRef]
45. He, Y.; Aliyu, A.; Evans, M.; Luo, C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *J. Med. Internet Res.* **2021**, *23*, e21747. [CrossRef]
46. Argaw, S.T.; Troncoso-Pastoriza, J.R.; Lacey, D.; Florin, M.-V.; Calcavecchia, F.; Anderson, D.; Burleson, W.; Vogel, J.-M.; O'leary, C.; Eshaya-Chauvin, B.; et al. Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 146. [CrossRef]
47. Kruse, C.S.; Frederick, B.; Jacobson, T.; Monticone, D.K. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technol. Health Care* **2017**, *25*, 1–10. [CrossRef]
48. Coventry, L.; Branley, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas* **2018**, *113*, 48–52. [CrossRef]
49. Giansanti, D. Cybersecurity and the digital-health: The challenge of this millennium. *Healthcare* **2021**, *9*, 62. [CrossRef] [PubMed]
50. Jalali, M.S.; Razak, S.; Gordon, W.; Perakslis, E.; Madnick, S. Health care and cybersecurity: Bibliometric analysis of the literature. *J. Med. Internet Res.* **2019**, *21*, e12644. [CrossRef] [PubMed]
51. Niki, O.; Saira, G.; Arvind, S.; Mike, D. Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. *Digit. Health* **2022**, *8*, 20552076221104665. [CrossRef] [PubMed]
52. Lehne, M.; Sass, J.; Essenwanger, A.; Schepers, J.; Thun, S. Why digital medicine depends on interoperability. *NPJ Digit. Med.* **2019**, *2*, 79. [CrossRef] [PubMed]
53. Martin, L.T.; Nelson, C.; Yeung, D.; Acosta, J.D.; Qureshi, N.; Blagg, T.; Chandra, A. The issues of interoperability and data connectedness for public health. *Big Data* **2022**, *10*, S19–S24. [CrossRef]
54. Torab-Miandoab, A.; Samad-Soltani, T.; Jodati, A.; Rezaei-Hachesu, P. Interoperability of heterogeneous health information systems: A systematic literature review. *BMC Med. Inform. Decis. Mak.* **2023**, *23*, 18. [CrossRef] [PubMed]
55. Hussein, R.; Wurhofer, D.; Strumegger, E.M.; Stainer-Hochgatterer, A.; Kulnik, S.T.; Crutzen, R.; Niebauer, J. General Data Protection Regulation (GDPR) toolkit for digital health. *Stud. Health Technol. Inform.* **2022**, *290*, 222–226. [PubMed]
56. Torous, J.; Stern, A.D.; Bourgeois, F.T. Regulatory considerations to keep pace with innovation in digital health products. *NPJ Digit. Med.* **2022**, *5*, 121. [CrossRef]
57. Rodriguez-Villa, E.; Torous, J. Regulating digital health technologies with transparency: The case for dynamic and multi-stakeholder evaluation. *BMC Med.* **2019**, *17*, 226. [CrossRef]
58. Brall, C.; Schröder-Bäck, P.; Maeckelberghe, E. Ethical aspects of digital health from a justice point of view. *Eur. J. Public Health* **2019**, *29* (Suppl. S3), 18–22. [CrossRef]
59. Zarif, A. The ethical challenges facing the widespread adoption of digital healthcare technology. *Health Technol.* **2022**, *12*, 175–179. [CrossRef]
60. Maeckelberghe, E.; Zdunek, K.; Marceglia, S.; Farsides, B.; Rigby, M. The ethical challenges of personalized digital health. *Front. Med.* **2023**, *10*, 1123863. [CrossRef]
61. Jarva, E.; Oikarinen, A.; Andersson, J.; Tuomikoski, A.M.; Kääriäinen, M.; Meriläinen, M.; Mikkonen, K. Healthcare professionals' perceptions of digital health competence: A qualitative descriptive study. *Nurs. Open* **2022**, *9*, 1379–1393. [CrossRef]
62. Wubante, S.M.; Tegegne, M.D. Health professionals knowledge of telemedicine and its associated factors working at private hospitals in resource-limited settings. *Front. Digit. Health* **2022**, *4*, 976566. [CrossRef] [PubMed]
63. Ghaddaripouri, K.; Mousavi Baigi, S.F.; Abbaszadeh, A.; Mazaheri Habibi, M.R. Attitude, awareness, and knowledge of telemedicine among medical students: A systematic review of cross-sectional studies. *Health Sci. Rep.* **2023**, *6*, e1156. [CrossRef]

64. Duggal, M.; El Ayadi, A.; Duggal, B.; Reynolds, N.; Bascaran, C. Editorial: Challenges in implementing digital health in public health settings in low and middle income countries. *Front. Public Health* **2023**, *10*, 1090303. [CrossRef] [PubMed]
65. Hadjiat, Y. Healthcare inequity and digital health-a bridge for the divide, or further erosion of the chasm? *PLoS Digit. Health* **2023**, *2*, e0000268. [CrossRef]
66. Seh, A.H.; Zarour, M.; Alenezi, M.; Sarkar, A.K.; Agrawal, A.; Kumar, R.; Ahmad Khan, R. Healthcare data breaches: Insights and implications. *Healthcare* **2020**, *8*, 133. [CrossRef]
67. Koczkodaj, W.W.; Masiak, J.; Mazurek, M.; Strzałka, D.; Zabrodskii, P.F. Massive health record breaches evidenced by the Office for Civil Rights data. *Iran. J. Public Health* **2019**, *48*, 278–288. [CrossRef]
68. Williams, P.A.; Woodward, A.J. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Med. Devices* **2015**, *8*, 305–316. [CrossRef]
69. Ransford, B.; Kramer, D.B.; Kune, D.F.; de Medeiros, J.A.; Yan, C.; Xu, W.; Crawford, T.; Fu, K. Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists. *Pacing. Clin. Electrophysiol.* **2017**, *40*, 913–917. [CrossRef]
70. Priestman, W.; Anstis, T.; Sebire, I.G.; Sridharan, S.; Sebire, N.J. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health Care Inform.* **2019**, *26*, e100031. [CrossRef]
71. Abdelhamid, M. The role of health concerns in phishing susceptibility: Survey design study. *J. Med. Internet Res.* **2020**, *22*, e18394. [CrossRef] [PubMed]
72. Gordon, W.J.; Wright, A.; Aiyagari, R.; Corbo, L.; Glynn, R.J.; Kadakia, J.; Kufahl, J.; Mazzone, C.; Noga, J.; Parkulo, M.; et al. Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Netw. Open* **2019**, *2*, e190393. [CrossRef] [PubMed]
73. Chapman, P. Are your IT staff ready for the pandemic-driven insider threat? *Netw. Secur.* **2020**, *2020*, 8–11. [CrossRef]
74. Khan, N.; JHoughton, R.; Sharples, S. Understanding factors that influence unintentional insider threat: A framework to counteract unintentional risks. *Cogn. Technol. Work* **2022**, *24*, 393–421. [CrossRef]
75. Yeo, L.H.; Banfield, J. Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspect Health Inf. Manag.* **2022**, *19*, 1i. [PubMed]
76. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors* **2021**, *21*, 5119. [CrossRef] [PubMed]
77. Neprash, H.T.; McGlave, C.C.; Cross, D.A.; Virnig, B.A.; Puskarich, M.A.; Huling, J.D.; Rozenshtein, A.Z.; Nikpay, S.S. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum.* **2022**, *3*, e224873. [CrossRef] [PubMed]
78. Dameff, C.; Tully, J.; Chan, T.C.; Castillo, E.M.; Savage, S.; Maysent, P.; Hemmen, T.M.; Clay, B.J.; Longhurst, C.A. Ransomware Attack associated with disruptions at adjacent emergency departments in the US. *JAMA Netw. Open* **2023**, *6*, e2312270. [CrossRef] [PubMed]
79. Argaw, S.T.; Bempong, N.E.; Eshaya-Chauvin, B.; Flahault, A. The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. *BMC Med. Inform. Decis. Mak.* **2019**, *19*, 10. [CrossRef]
80. Borky, J.M.; Bradley, T.H. Protecting information with cybersecurity. *Eff. Model-Based Syst. Eng.* **2018**, 345–404. [CrossRef]
81. Almalawi, A.; Khan, A.I.; Alsolami, F.; Abushark, Y.B.; Alfakeeh, A.S. Managing security of healthcare data for a modern healthcare system. *Sensors* **2023**, *23*, 3612. [CrossRef]
82. Sarosh, P.; Parah, S.A.; Bhat, G.M. An efficient image encryption scheme for healthcare applications. *Multimed. Tools Appl.* **2022**, *81*, 7253–7270. [CrossRef]
83. Hijji, M.; Alam, G. Cybersecurity Awareness and Training (CAT) framework for remote working employees. *Sensors* **2022**, *22*, 8663. [CrossRef]
84. Arain, M.A.; Tarraf, R.; Ahmad, A. Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *J. Multidiscip Health* **2019**, *12*, 73–81. [CrossRef] [PubMed]
85. Kamerer, J.L.; McDermott, D.S. Cyber hygiene concepts for nursing education. *Nurse Educ. Today* **2023**, *130*, 105940. [CrossRef] [PubMed]
86. Rubia, F.; Affan, Y.; Lin, L.; Jianmin, W. How persuasive is a phishing email? A phishing game for phishing awareness. *J. Comp. Secur.* **2019**, *27*, 581–612.
87. Johansson, D.; Jönsson, P.; Ivarsson, B.; Christiansson, M. Information technology and medical technology personnel's perception regarding segmentation of medical devices: A focus group study. *Healthcare* **2020**, *8*, 23. [CrossRef] [PubMed]
88. Zarour, M.; Alenezi, M.; Ansari, M.T.J.; Pandey, A.K.; Ahmad, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Ensuring data integrity of healthcare information in the era of digital health. *Health Technol. Lett.* **2021**, *8*, 66–77. [CrossRef] [PubMed]
89. Seo, H.J.; Kim, H.H.; Kim, J.H. A SWOT analysis of the various backup scenarios used in electronic medical record systems. *Health Inform. Res.* **2011**, *17*, 162–171. [CrossRef]
90. Mallinder, J.; Drabwell, P. Cyber security: A critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber attack. *J. Bus. Contin. Emer. Plan* **2014**, *7*, 103–111.