Navigating Digital Health Technology: A Comprehensive Review of USFDA Regulations

Abstract

Digital health technology is revolutionizing the healthcare landscape by leveraging digital and information technologies to enhance healthcare delivery, monitoring and management. This technology encompasses a wide range of tools, including mobile apps, wearable, telemedicine, electronic health records, and AI-driven diagnostics. Digital health technologies may be beneficial but also problematic. Development requires navigating complicated regulatory systems and meeting changing criteria. These technologies, particularly those using AI algorithms, need robust clinical validation to prove their safety and usefulness. Health data is delicate; thus, privacy and security are crucial. Successful adoption requires interoperability with current healthcare systems, seamless user experience, and ethical and legal considerations. To maximize digital health technology's potential, clinical evidence, financial management, and change resistance must be addressed. Addressing these issues requires collaboration between healthcare professionals, technology professionals, regulators, and patients. Digital health technology can empower people, enhance patient outcomes, and transform healthcare by balancing innovation and safety. Despite challenges, digital health technology improves global health, needing continuing innovation, regulatory compliance, and equal access. This review provides a comprehensive analysis of the US Food and Drug Administration (USFDA) regulations governing digital health technologies, including, classification of DHT, mobile health applications, wearables, Cyber security, Regulatory expectations and challenges.

Keywords:

Digital health technology, USFDA regulations,AI-driven diagnostics, safety, medical devices, Cybersecurity, mHealth

INTRODUCTION:

The broad scope of digital health includes categories such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine.From mobile medical apps and software that support the clinical decisions doctors make every day to artificial intelligence and machine learning, digital technology has been driving a revolution in health care. Digital health tools have the vast potential to improve our ability to accurately diagnose and treat disease and to enhance the delivery of health care for the individual[1].The “triple aim” of healthcare reform provides namely:

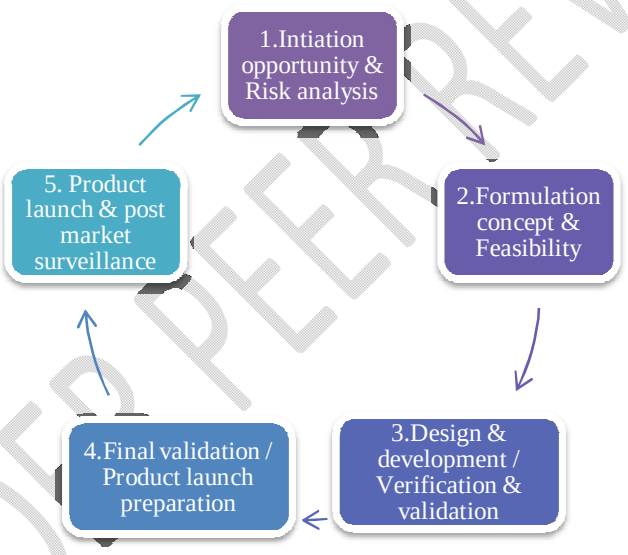
- **i)** improving the quality, safety, and experience of care
- **ii)** enhancing population health
- **iii)** reducing per capita costs of healthcare[2].

The field of influencing or changing human behaviour through digital technologies started with the term persuasive technology (PT) around 1998. It states that persuasion is more than just computer-mediated communication but focuses on human-computer interaction. He defined PT as “how people can be persuaded

when interacting with the technology and adjusting itself according to the actions, inputs, and context of persuaded party.Over time, many terms have emerged to describe technology-based behaviour change interventions[3].Ithas been argued that the capacity to collect, store, and analyze extensive amounts of health data is the chief driving force of digital health. The accessibility of such data is rejuvenating the process involved in diagnosing, managing, and treating disease, thus exceeding the conventional boundaries of how health care institutions and providers operate. A case in point is the myriad number of smartphone apps that allow patients to seamlessly monitor various aspects of their health care beyond the confines of a health care institution[4].

Digital health technologies use computing platforms, connectivity, software, and sensors for health care and related uses.Development of Medical Devices related to Digital Health Technologies represented in **Fig 1**.

Fig .1 Digital Health Technologies



They include technologies intended for use as a medical product, in a medical product, as companion diagnostics, or as an adjunct to other medical products (devices, drugs, and biologics). They may also be used to develop or study medical products[5].Digital health technologies (DHTs), pharmacogenomics and process innovations are rapidly emerging as promising health interventions. The technological and industry-structural differences between DHTs and traditional medical devices are summarized in **Table No 1**.

Table 1 :Technological and industry-structural differences between DHTs and traditional medical devices

Technology component	**Industry-structural component**

➢ Adaptability ➢ New entrants ➢ Variety ➢ Novelty ➢ Accessibility	➢ New entrants ➢ Changing roles ➢ New delivery models

More innovations are expected to emerge as healthcare demand and spending rise. Nevertheless, many of these breakthroughs have not reached the healthcare providers and the people most in need to tackle the rising burden of diseases[6].Current health care delivery models are largely based on a top-down medical model, driven by the World Health Organization, with doctors and nurses as the purveyors of knowledge and the arbiters of care. Care is primarily accessed through health facilities whether at the hospital or in the community, and information is delivered primarily by medical personnel[7]. Consumer technology companies, such as Apple, Google, and Fitbit, have entered the healthcare market, and thousands of health or fitness mobile apps are in the Apple App Store and Google Play, though only a small proportion have been approved by entities such as the FDA[8].

Benefits of digital health technologies:

Digital technologies enable consumers to have more control over their health and provide practitioners with a more complete view of patient health via data access. There is considerable potential for digital health to increase efficiency and improve medical outcomes. With the use of these technologies, patients may be able to make more informed decisions about their health and have access to new options for treatment of chronic diseases, early identification of life-threatening illnesses, and prevention outside of traditional medical settings[9].Digital health technology is being used by providers and other stakeholders in order to improve patient care customization, increase quality, decrease costs, and improve access. The use of technology, including social media, internet applications, and mobile phones, is not only changing the way we communicate but also opening up new avenues for monitoring our health and wellbeing and improving our ability to gain information[10].Digital health technologies are becoming widely adopted in major healthcare systems, including the US, because to the potential benefits they may provide to payers, physicians, and patients. The sector got venture capital funding of over 29.1 billion USD in 2021, compared to 14.9 billion in 2020 and 8.2 billion in 2019.The industry's high level of investment activity and non-startups' R and D expenditure are consistent with the production of a vast quantity of items. Over 318 000 health-related apps were available in app stores

throughout the globe as of 2017. The FDA has approved 64 AI/ML-based digital health devices for commercialization by 2020. The advantages for patients and healthcare systems are not as evident as they might be, even if use by physicians and patients is growing in tandem with consumer-focused digital health devices and beyond[11].

Effects on quality and safety:

Health information technology increases adherence to protocol- or guideline-based care, which has a substantial effect on the quality of treatment. Decision support was a feature of all adherence studies, and it was often given in the form of electronic reminders. Automated provider order entry systems or electronic health records often included decision assistance features. Physician order-entry systems were more often assessed in the context of an inpatient stay, whereas electronic health record systems were more frequently examined in the outpatient setting[12].In order to use electronic health record (EHR) technology to identify, measure, and enhance the quality and safety of the care they provide, healthcare organizations and their EHR providers must work together to monitor and optimize this technology. Enhancing the general security of our expanding healthcare system is an enormous sociotechnical undertaking[13].

CLASSIFICATION OF DIGITAL HEALTH TECHNOLOGIES BASED ON RISK:

Digital health technologies are classed according to the danger they bring to patients, healthcare practitioners, and the whole healthcare system. Here's a breakdown of digital health technology into three risk categories: low, moderate, and high.

1. Low-Risk Digital Health Technologies:

These technologies typically involve collecting and transmitting basic health information and are unlikely to cause significant harm if they malfunction or provide inaccurate data.

Examples:Health and fitness apps for tracking physical activity, sleep, and nutrition. Wellness and meditation apps.

2. Moderate-Risk Digital Health Technologies:

These technologies involve more complex functions, such as medical diagnosis, treatment recommendations, and remote monitoring of patients with chronic conditions. Malfunctions or inaccuracies could have a moderate impact on patient health.

Examples: Remote monitoring devices for chronic conditions (e.g., heart rate monitors for cardiac patients) and Medication reminder apps.

3. High-Risk Digital Health Technologies:

In the event of a malfunction or inaccurate result, these technologies might have a major influence on the health and safety of patients. They often involve critical medical decisions.

Examples: Implantable medical devices with remote connectivity (e.g., pacemakers, insulin pumps). Remote surgery or robotic surgical systems[14].

It is important to note that while this classification provides a general guideline, the level of risk can also depend on factors such as the specific technology's design, regulatory approvals, intended use, and the training and expertise of healthcare providers using the technology.

USFDA GUIDELINES ON DIGITAL HEALTH TECHNOLOGIES:

FDA provides 24 guidance documents regarding digital health technologies[15]. At present circumstances,out of these 21 are final documents and the remaining 3 are draft status (Not for Implementation, contains non-binding recommendations) listed in **Table No 2**.

Table 2 :USFDA Guidelines On Digital Health Technologies

S. No	The guidance documents
1.	Cyber security for Networked Medical Devices Containing Off-the-Shelf (OTS) Software.
2.	Information for Healthcare Organizations about FDA's "Guidance for Industry: Cyber security for Networked Medical Devices Containing Off-The-Shelf (OTS) Software"
3.	Guidance: Acceptable Media for Electronic Product User Manuals.
4.	Radio Frequency Wireless Technology in Medical Devices.
5.	Content of Premarket Submissions for Management of Cyber security in Medical Devices.
6.	Applying Human Factors and Usability Engineering to Medical Devices.

7.	Post market Management of Cyber security in Medical Devices.
8.	Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices.
9.	Deciding When to Submit a 510(k) for a Software Change to an Existing Device.
10.	Software as a Medical Device (SAMD): Clinical Evaluation.
11.	Medical Device Accessories - Describing Accessories and Classification Pathways.
12.	Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act.
13.	Off-the-Shelf Software Use in Medical Devices.
14.	General Wellness: Policy for Low-Risk Devices
15.	Multiple Function Device Products: Policy and Considerations.
16.	Digital Health Technologies for Remote Data Acquisition in Clinical Investigation. (Draft)
17.	Cyber security in Medical Devices: Quality System Considerations and Content of Premarket Submissions. (Draft)
18.	Clinical Decision Support Software.
19.	Policy for Device Software Functions and Mobile Medical Applications
20.	Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices.
21.	Computer-Assisted Detection Devices Applied to Radiology Images and Radiology Device Data - Premarket Notification [510(k)] Submissions.
22.	Clinical Performance Assessment: Considerations for Computer-Assisted Detection Devices Applied to Radiology Images and Radiology Device Data 10 Premarket Approval (PMA) and Premarket Notification [510(k)] Submissions.
23.	Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Function. (Draft)
24.	Content of Premarket Submissions for Device Software Functions

Digital health terms:

1. Software designed for medical applications that may run on a range of virtual environments and operating systems is known as Software as a Medical Device, or SaMD. If the software powers or manages the hardware medical device, it is not considered a SaMD[16]. This includes standalone programs for desktop computers and mobile platforms like tablets and smartphones.

2. Advanced Analytics:A device or technique that can recognize, evaluate, and make use of large, complex data sets from several sources. The product gathers new and pertinent data or patterns for use in applications related to medicine. Statistical modeling and analytical techniques that provide predictions, insights, and suggestions based on the analysis may be used in advanced analytics[17].

3. Cloud: The term "cloud" refers to an internet-based device or product that provides computing resources and data on demand. It consists of computer networks, servers, storage, applications, and services, such as operating systems, software, applications, and storage devices.

4. Cybersecurity and Interoperability: An apparatus or product that can stop illegal access, alteration, abuse, or denial of service, as well as the unlawful use of data that is sent, stored, or accessed from a medical device to a third party. Interoperability is the capacity of a product or device to communicate and utilize data with another medical or non-medical product, system, or device via an electronic interface [18].The capacity of several systems, devices, apps, or products to link and interact in a coordinated manner, requiring no effort from the end user.

5.Medical Device Data System (MDDS): Hardware or software that may transfer, store, transform data formats, or show data from medical devices without affecting the parameters or operation of any connected medical devices [19].

6. Mobile Medical App (MMA): Software functions (often mobile applications) that change a mobile platform into a regulated medical device by using display screens, attachments, or features comparable to those of presently regulated medical devices must comply with the device classification associated with the converted platform[20].

By connecting to one or more medical devices, they act as an extension of those devices, allowing for data analysis or control of the device(s).

Legal framework for data privacy and cybersecurity:

Among the most contentious issues in the discussion of digital health technologies are privacy and data security. The ability of enormous data systems to secure sensitive information has been brought into doubt by recent data breaches at major corporations like Sony, Equifax, and Amazon[21].In the United States, federal rules controlling consumer data privacy are segmented, and their applicability is determined by the status of the company involved, the kind of data, and the impacted population. In addition, several states have their own privacy regulations that go beyond federal obligations.

US state laws and regulatory guidance:

Many US states have data privacy laws. In mid-2017, five states were developing biometric methods that included fingerprints, face characteristics, DNA, eye or iris identification, and voicerecognition. Breach notification laws are another state action. HIPAA mandates disclosure to the OCR and, in certain cases, the affected individual(s) if specific PHI is compromised, but there is no federal breach reporting requirement. However, breach notification laws requiring businesses or governmental organizations to notify people about personally identifiable information security breaches exist in 48 US states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands. Security breach legislation often include reporting requirements, exclusions (like encrypted data), breaches, compliance, and definitions of "personal information" (like name and social security number). Notifying about a breach may soon become difficult. If the notification requirement is satisfied, the organization must identify all applicable laws in all relevant countries and inform all impacted individuals [22].

REGULATORY EXPECTATIONS OVER DIGITAL HEALTH TECHNOLOGIES:

This regulatory expectation depends on factors such as the type of technology, its intended use, its level of risk, and the regulatory body overseeing the region.

1. Risk Classification: Digital health technologies are often categorized by regulatory bodies according to the degree of danger they pose to users and patients. Higher-risk technologies, such as AI-driven diagnostic tools or implantable devices, typically face more stringent regulatory requirements compared to lower-risk technologies like fitness tracking apps.

2. Quality Management Systems: Regulatory bodies generally expect manufacturers and developers of digital health technologies to implement robust quality management systems that ensure the consistent design, development, and manufacturing of safe and effective products[23].

3. Clinical Evidence: For medical devices and technologies with a medical purpose, regulatory agencies may require clinical evidence demonstrating the safety, performance, and efficacy of the product. This could involve clinical trials, real-world data collection, and validation studies.

4. Software Validation: Regulatory bodies often demand validation procedures for software-based technologies to make sure the program works as intended and satisfies the criteria for its intended usage [24]. This involves putting accuracy, dependability, and usability via testing.

5. User Training and Education: Clear instructions for use, user training, and educational materials are expected to ensure that users, including healthcare professionals and patients, can use the technology safely and effectively.

6. Labeling and Instructions for Use: Clear and accurate labeling and instructions for use are crucial for both users and regulators to understand the intended purpose, limitations, and proper usage of the technology.

7. Global Harmonization: For technologies intended for international markets, regulatory expectations may involve harmonizing with global standards and regulations to facilitate market access and ensure consistent quality[25].

8. Transparency and Reporting: Manufacturers are generally expected to maintain open and transparent communication with regulatory agencies, promptly reporting any safety concerns, adverse events, or changes in product status.

Keep in mind that these are general regulatory expectations, and the specifics can vary depending on the regulatory body (such as the FDA in the United States, the European Medicines Agency in the EU)

CHALLENGES FACED DURING THE DEVELOPMENT OF DIGITAL HEALTH TECHNOLOGY:

The process of developing digital health technology is dynamic, intricate, and fraught with difficulties of its own. These are a few typical obstacles encountered while developing digital health technologies:

1. Regulatory Compliance: Navigating the regulatory landscape for medical devices and health technologies can be challenging. Ensuring that the technology complies with the relevant regulations and standards, and meeting documentation requirements can be time-consuming and complex.

2. Data Privacy and Security: Robust data privacy and security is essential for digital health devices that manage sensitive health data. Thorough preparation and execution of security measures are necessary to comply with strict data protection laws and prevent data breaches.

3. Clinical Validation: Extensive clinical validation is often necessary to demonstrate the safety and effectiveness of medical innovations[26]. Designing and conducting appropriate clinical trials or studies can be resource-intensive and may present challenges related to participant recruitment, data collection, and interpretation.

4. Interoperability: It may be difficult to integrate digital health technology with current healthcare systems and guarantee interoperability because of variations in protocols, standards, and data formats. Lack of interoperability can hinder data exchange and seamless workflow integration.

5.Accuracy and Reliability: Ensuring the accuracy and reliability of digital health technologies, especially those involving diagnostic or monitoring capabilities, is critical. Algorithms and sensors must be well-calibrated and validated to avoid misdiagnoses or false readings.

6. Technical Challenges: Complex software, hardware, and connection solutions might provide technical difficulties in the form of compatibility problems, software defects, and guaranteeing consistent performance across many platforms and devices.

7. Healthcare Professional Adoption: Persuading medical personnel to accept and incorporate new technology into their workflow might present difficulties. Adoption may be hampered by a lack of knowledge with the advantages of the technology, resistance to change, and worries about additional strain.

8. Cost and Reimbursement: Digital health technologies may face challenges related to reimbursement by healthcare systems or insurance providers. Demonstrating the economic value and cost-effectiveness of the technology can be important for securing reimbursement[27].

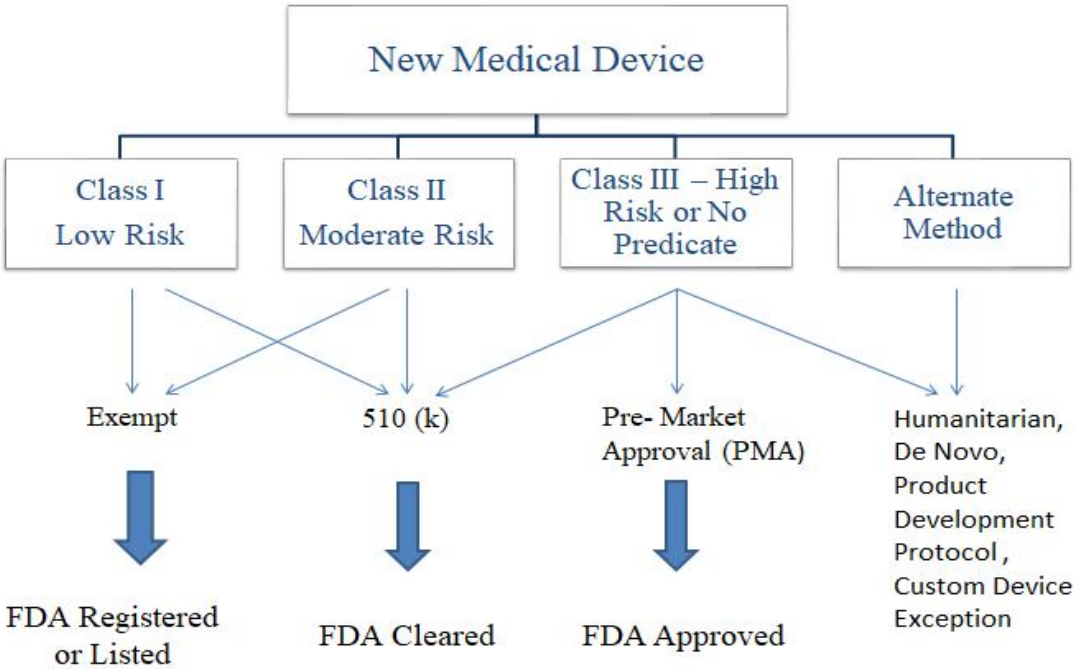
9. Ethical and Legal Considerations: Digital health technologies can raise ethical concerns related to data ownership, consent, and potential biases in AI algorithms. Adhering to ethical guidelines and addressing legal considerations is important for maintaining trust.

APPROVAL PROCEDURE FOR MEDICAL DEVICES AS PER USFDA

In order to ensure the safety, efficacy, and regulatory compliance of medical devices linked to digital health technologies, a number of procedures make up the clearance process. Depending on the category of the equipment and the location, different methods apply. A general overview of the US Food and Drug Administration's (FDA) approval procedure for medical devices is provided here:

1**. Device categorization:**Based on the planned use and degree of risk, classify the gadget appropriately. Depending on how dangerous they are, medical devices are categorized into three classes (Class I, II, and III).The approval process for Medical Devices related to Digital Health Technologies in **Fig 2**.

Fig .2 Approval process for Medical Devices related to Digital Health Technologies



a) Class I Devices: These devices are deemed low risk and do not typically need FDA premarket approval.

b) Class II Devices: These devices are referred to as Moderate risk-based medical devices. Most digital health devices fall into this category. Manufacturers typically submit a 510(k) premarket notification.

c) Class III Devices: These devices are considered higher risk-based, such as implantable devices, and require a more rigorous premarket approval (PMA) application.

2. Pre-market notification (510(k)) and premarket approval (PMA): 510(k) - The device to be sold must demonstrate to the FDA that it is at least as safe and effective as the legally marketed product—which is not subject to premarket clearance—through a premarket application.

PMA - Scientific and regulatory documentation submitted to the FDA demonstrating the safety and effectiveness of a Class III device. A PMA application involves administrative components, but excellent research and scientific writing are essential for approval.

3. De Novo Classification: Manufacturers may file a De Novo application if their unique gadget lacks an appropriate predicate device. This process is used to establish the device's classification and determine appropriate regulatory requirements.

4. Clinical Data: Depending on the device's classification and intended use, clinical data may be required to demonstrate safety and efficacy. This can involve conducting clinical trials or studies to gather evidence.

5. Quality System Regulations (QSR): Manufacturers are required to establish and maintain a quality system that complies with FDA's Quality System Regulation (QSR) to ensure proper design, development, manufacturing, and control of the device[28].

6. Data Submission: Prepare and submit the necessary documentation to the FDA, including the 510(k) submission, PMA application, De Novo application, and other relevant documents such as labeling, risk assessments, and clinical data.

7. FDA Review and Decision: The FDA reviews the submitted data and conducts a thorough evaluation of the device's safety, efficacy, and compliance with regulatory requirements. Based on the review, the FDA will issue

a decision, which can include clearance (for 510(k)) or approval (for PMA or De Novo), or a request for additional information. The decision is typically communicated to the manufacturer in writing.

8. Post-Market Requirements: Once the item has been authorized or cleared, manufacturers are responsible for post-market monitoring, adverse event reporting, and assuring continuing compliance with regulatory criteria [29].

It is crucial to remember that this method is just a broad overview and may not include all conceivable circumstances. Different countries have their regulatory agencies and processes for medical device approval.

CONCLUSIONS:

Digital health technology has enormous potential for revolutionizing healthcare delivery, increasing patient outcomes, and boosting people' overall health and wellbeing. However, its development and adoption are not without challenges. From navigating complex regulatory landscapes to ensuring data privacy, clinical validation, and user acceptance, the journey to realizing the potential of digital health is marked by a range of hurdles.Addressing these issues needs a comprehensive and collaborative effort that includes healthcare professionals, technology innovators, regulatory organizations, lawmakers, patients, and other stakeholders.By focusing on robust clinical validation, user-centered design, ethical considerations, and interoperability standards, the development of digital health technologies can yield solutions that are not only innovative but also safe, effective, and accessible to diverse populations.As digital health technologies continue to evolve and become more integrated into healthcare systems, the lessons learned from addressing challenges will contribute to a more informed, resilient, and patient-centric approach to shaping the future of healthcare. With careful consideration, collaboration, and a commitment to ethical and effective solutions, digital health technology can indeed revolutionize healthcare for the better.

REFERENCES

1. Sarbadhikari SN. The role of standards for digital health and health information management. J. Basic Clin. Res. (JBCR). 2019;6(1):1.
2. Aziz Sheikh, Harpreet S Sood, David W Bates. Leveraging health information technology to achieve the “triple aim” of healthcare reform. Journal of the American Medical Informatics Association.2015;22(4):849-856.
3. Fawad Taj, Michel C A Klein, Aart van Halteren.Digital Health Behavior Change Technology :Bibliography and scoping Review of Two Decades of Research
4. Afua Adjekum, Alessandro Blasimme, Effy Vayena. Elements of Trust in Digital Health Systems: Scoping Review.Journal of Medical Internet Research.2018;(12)**:** e11254.

5. https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health
6. Jeffrey David Iqbal,Nikola Biller-Andorno,the regulatory gap in digital health and alternative pathways to bridge it.Health Policy and Technology.2022;11(3):100663.
7. Marc Mitchell, Lena Kan.Digital Technology and the Future of Health Systems. Health care System &Reforms.2019;5(2):113–120.
8. RongziShan, Sudipa Sarkar,Seth S. Martin. Digital health technology and mobile devices for the management of diabetes mellitus: state of the art.2019;62: 877-887.
9. Voelker R. New center at FDA will advance digital health innovation. JAMA. 2020;324(17):1715.
10. Awad A, Trenfield SJ, Pollard TD, Ong JJ. Connected healthcare: Improving patient care using digital health technologies. Advanced Drug Delivery Reviews. 2021; 178:113958.
11. TsegahunManyazewal, YimtubezinashWoldeamanuel, Henry M. Blumberg, Abebaw Fekadu & Vincent C. Marconi. The potential use of digital health technologies in the African context: a systematic review of evidence from Ethiopia. npj Digital Medicine.2021;4:125.
12. Basit Chaudry MD,Jerome Wang,MD,Shinyi Wu,Margaret Maglione, MPP; Walter Mojica, MD; Elizabeth Roth, MA; Sally C. Morton, PhD; Paul G. Shekelle, MD, PhD. Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care. Annals of internal Medicine.2006;144(10):742-752.
13. Dean F Sittig, Adam Wright and Hardeep Singh. Current challenges in health information technology–related patient safety. Health Informatics Journal.2018;26(1):181-189.
14. Nwe K, Larsen ME, Nelissen N, Wong DC. Medical mobile app classification using the National Institute for Health and Care Excellence evidence standards framework for digital health technologies: interrater reliability study. Journal of Medical Internet Research. 2020;22(6): e17457.
15. https://www.fda.gov/medical-devices/digital-health-center-excellence
16. Food and Drug Administration, 2019. Proposed regulatory framework for modifications to artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD)
17. Dash S, Shakyawar SK, Sharma M, Kaushik S.Big data in healthcare: management, analysis and prospects. Journal of big data. 2019;6(1):1-25.
18. Katzis K, Jones RW, Despotou G. The challenges of balancing safety and security in implantable medical devices. InUnifying the Applications and Foundations of Biomedical and Health Informatics.2016:25-28
19. McHugh M, McCaffery F, Casey V. US FDA releases final rule on medical device data systems: what does this mean for device manufacturers.
20. YetisenAK, Martinez-Hurtado JL, da Cruz Vasconcellos F, Simsekler ME, Akram MS, Lowe CR. The regulation of mobile medical applications. Lab on a Chip. 2014;14(5):833-40.
21. Abhinav Sharma, MD,a,b,cRobert A. Harrington, MD,cMark B. McClellan, MD, PHD,Mintu P. Turakhia, MD, MA.Using Digital Health Technologyto Better Generate Evidence and Deliver Evidence-Based Care.Journal of the American college of Cardiology.2018;71(23):2680-90.
22. SvetlanaLyapustina, Katherine Armstrong. Regulatory considerations for cybersecurity and data privacy in digital health and medical application and products. CSC .2018

23. Larson, D.B., Harvey, H., Rubin, D.L., Irani, N., Justin, R.T. and Langlotz, C.P.,. Regulatory frameworks for development and evaluation of artificial intelligence–based diagnostic imaging algorithms: summary and recommendations. Journal of the American College of Radiology.2021;18(3):413-424.
24. Carroll N, Richardson I. Software-as-a-medical device: demystifying connected health regulations. Journal of Systems and Information Technology. 2016;18(2):186-215.
25. Cheng M. Medical device regulations: global overview and guiding principles.
26. Thapa C, Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine. 2021;129: 104130.
27. Kelley LT, Fujioka J, Liang K, Cooper M, Jamieson T, Desveaux L. Barriers to creating scalable business models for digital health innovation in public systems: qualitative case study. JMIR Public Health and Surveillance. 2020;6(4):e20579.
28. Kinsel D. Design control requirements for medical device development. World Journal for Pediatric and Congenital Heart Surgery. 2012;3(1):77-81.
29. BadnjevićA, Pokvić LG, Deumic A, Becirovic LS. Post-market surveillance of medical devices: A review. Technology and Health Care. 2022(Preprint):1-5.