IJBPAS, September, 2024, 13(9): 4397-4408

ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)

'A Bridge Between Laboratory and Reader'

www.ijbpas.com

A COMPREHENSIVE REVIEW OF DIGITAL HEALTH TECHNOLOGY REGULATION AS PER USFDA

CHANDRU S, SUDHEER KUMAR T* AND KAMARAJ R

Department of Pharmaceutical Regulatory Affairs, SRM College of Pharmacy, SRM Institute of Science and Technology, Kattankulathur- 603203, Chengalpattu, Tamil Nadu, India

***Corresponding Author: Mr. T. Sudheer Kumar: E Mail: tirumals@srmist.edu.in**

Received 18th July 2023; Revised 20th Sept. 2023; Accepted 2nd Dec. 2023; Available online 1st Sept. 2024

https://doi.org/10.31032/IJBPAS/2024/13.9.8306

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. While promising significant benefits, the development of digital health technology presents several challenges. Navigating complex regulatory frameworks and ensuring compliance with evolving standards is a critical aspect of development. Robust clinical validation is required to establish the safety and efficacy of these technologies, especially for those employing AI algorithms. Data privacy and security are paramount due to the sensitive nature of health information. Interoperability with existing healthcare systems, seamless user experience, and addressing ethical and legal concerns are essential for successful adoption. The ability to generate substantial clinical evidence, manage costs, and overcome resistance to change are also key factors in realizing the potential of digital health technology. Collaboration among healthcare experts, technology professionals, regulatory bodies, and patients is crucial for addressing these challenges. By striking a balance between innovation and safety, digital health technology can empower individuals, improve patient outcomes, and reshape healthcare practices. While obstacles exist, the positive impact of digital health technology on global health is undeniable, requiring ongoing dedication to innovation, regulatory compliance, and equitable access.

Keywords: Mobile medical app, Cybersecurity, Software, mHealth, Wearables

INTRODUCTION

Digital Health

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]**.

Digital health technologies use computing platforms, connectivity, software, and sensors for health care and related uses. 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 **[2]**.

Benefits of Digital Health Technologies:

Digital tools are giving providers a more holistic view of patient health through access to data and giving patients more control over their health. Digital health offers real opportunities to improve medical outcomes and enhance efficiency. These technologies can empower consumers to make better-informed decisions about their own health and provide new options for facilitating prevention, early diagnosis of life-threatening diseases, and management of chronic conditions outside of traditional health care settings **[3]**. Providers and other stakeholders are using digital health technologies in their efforts to: improve access, reduce costs, increase quality, and make medicine more personalized for patients. The use of technologies, such as smart phones, social networks, and internet applications, is not only changing the way we communicate, but also providing innovative ways for us to monitor our health and well-being and giving us greater access to information **[4]**.

Classification of Digital Health Technologies based on Risk:

Digital health technologies can be classified based on the level of risk they pose to patients, healthcare providers, and the broader healthcare system. Here's a classification of digital health technologies into three risk categories: low risk, moderate risk, and high risk.

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), Medication reminder apps.

3. High-Risk Digital Health Technologies:

These technologies have the potential to significantly impact patient health and safety if they fail or provide incorrect information. They often involve critical medical decisions.

Examples: Implantable medical devices with remote connectivity (e.g., pacemakers, insulin pumps). Remote surgery or robotic surgical systems **[5]**.

It's 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. At present circumstances, out of these 21 are final documents and remaining 3 are draft status (Not for Implementation, contains non-binding recommendations). The guidance documents are intended to provide clarity on FDA's regulation of digital health products.

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 - 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 **[6]**.

Digital Health Terms:

1. Software as a Medical Device (SaMD): Software intended for one or more medical uses that may run on different operating systems or in virtual environments. Software run on a hardware medical device is a SaMD when not part of the intended use of the hardware medical device. Software is not SaMD if it drives or controls the hardware medical device **[7]**. This can include standalone software that is intended to run on general purpose computers or mobile platforms (that is, smartphone, tablet)
2. Advanced Analytics: A device or product that can identify, analyze, and use big data and large complex data sets from a variety of sources. The product extracts new and relevant information or patterns to use for medical purposes.

Advanced Analytics may include the use of statistical modelling and analytical techniques that provide insights, predictions, and recommendations based on its analysis **[8]**.

3.Cloud: A device or product with internet-based computing that provides computer processing resources and data on demand. The cloud is a shared pool of configurable resources (that is, computer networks, servers, storage, applications, and services). Computing and data storage resources include: servers, operating systems, networks, software, applications, services, and storage equipment.

4. Cyber security and Interoperability: A device or product that can prevent unauthorized access, modification, misuse, or denial of use, or the unauthorized use of information which is stored, accessed, or transferred from a medical device to an external recipient. A device or product that can exchange and use information through an electronic interface with another medical/non-medical product, system, or device is called as Interoperability **[9]**. the ability of different systems, devices, applications or products to connect and communicate in a coordinated way, without effort from the end user.

5. Medical Device Data System (MDDS): Hardware or software that can transfer, store, convert data formats, or display medical device data without controlling or altering the functions or parameters of any connected medical device **[10]**.

6.Mobile Medical App (MMA): Software function (typically mobile apps) that transform the mobile platform into a regulated medical device by using attachments , display screens, or by including functionalities similar to those of currently regulated medical devices are required to comply with the device classification associated with the transformed platform **[11]**.

These are an extension of one or more medical devices by connecting to such device(s) for the purpose of controlling the device(s) or analysing medical device data.

Regulatory Expectation over Digital Health Technologies:

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

1. Risk Classification: Regulatory agencies often classify digital health technologies based on their level of risk to patients and users. 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 **[12]**.

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: For software-based technologies, regulatory agencies often require validation processes to ensure that the software functions as intended and meets its intended use requirements **[13]**. This includes testing for accuracy, reliability, and usability.

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.

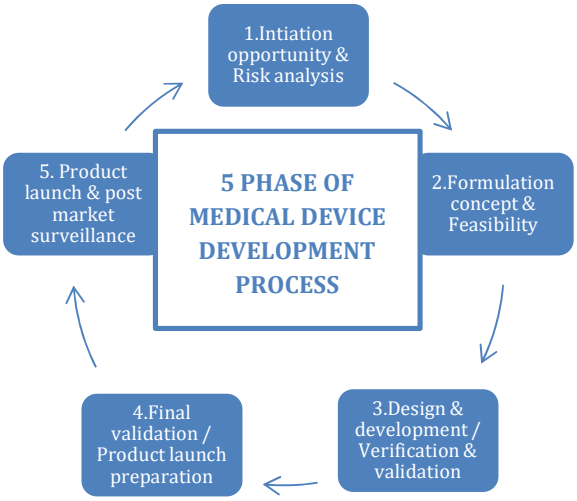
6. Labeling and Instructions for Use: Clear and accurate labeling and instructions for use are crucial for both users and regulators to understand the intended purpose, limitations, and proper usage of the technology.

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 **[14]**.

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 EU, etc.)

Development of Medical Device related to Digital Health Technologies:



Challenges faced during the development of Digital Health Technology:

The development of digital health technology is a dynamic and complex process that comes with its own set of challenges. Here are some common challenges faced during the development of digital health technology:

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: Digital health technologies handle sensitive health data, and ensuring robust data privacy and security is crucial. Meeting stringent data protection regulations and safeguarding against data breaches requires careful planning and implementation of security measures.

3. Clinical Validation: Demonstrating the safety and efficacy of medical devices and technologies often requires extensive clinical validation **[15]**. 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: Integrating digital health technologies with existing healthcare systems and ensuring interoperability can be challenging due to differences in data formats, standards, and protocols. 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.

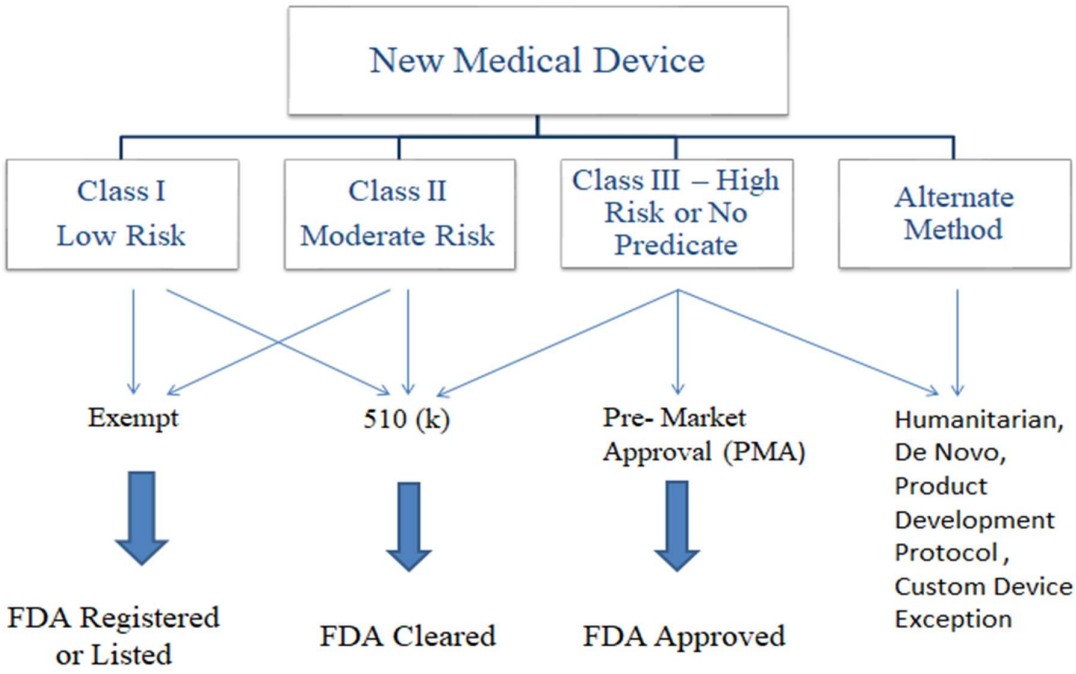
6. Technical Challenges: Developing and maintaining complex software, hardware, and connectivity solutions can encounter technical challenges, such as software bugs, compatibility issues, and ensuring consistent performance across different devices and platforms.

7. Healthcare Professional Adoption: Convincing healthcare professionals to adopt and integrate new technologies into their practice can be challenging. Resistance to change, concerns about increased workload, and unfamiliarity with the technology's benefits can hinder adoption.

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 **[16]**.

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 process for Medical Device related to Digital Health Technologies:



The approval process for medical devices related to digital health technologies involves several steps to ensure that the device is safe, effective, and compliant with regulatory requirements. The process can vary based on the region and the classification of the device. Here's a general overview of the approval process for medical devices in the United States, which is regulated by the U.S. Food and Drug Administration (FDA):

1.Device Classification: Determine the appropriate classification of the device based on its intended use and risk level. Medical devices are classified into three categories (Class I, II, or III) based on increasing levels of risk.

a) Class I Devices: These devices are considered low risk and generally do not require premarket submission to the FDA.

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

c) Class III Devices: These devices are considered as higher risk based , such as

implantable devices, require a more rigorous premarket approval (PMA) application.

2. Pre-Market Notification (510(k)) and Premarket Approval (PMA):

510(k) - Pre Market Submission made to the FDA to demonstrate that device to be marketed is at least as safe and effective that is subsequently equivalent to legally marketed device, that is not subject to premarket approval.

PMA - a scientific, regulatory documentation to FDA to demonstrate the safety and effectiveness of the Class III device. There are administrative elements of a PMA application, but good science and scientific writing is a key to the approval of PMA application.

3. De Novo Classification: For novel devices that do not have a suitable predicate device, manufacturers can submit a De Novo application. 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 **[17]**.

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 & 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 request for additional information. The decision is typically communicated to the manufacturer in writing.

8. Post-Market Requirements: Once the device is approved or cleared, manufacturers are responsible for post-market surveillance, adverse event reporting, and ensuring ongoing compliance with regulatory requirements.**[18]**

It's important to note that this process provides a general overview and may not cover all possible scenarios. Different countries have their own regulatory agencies and processes for medical device approval.

CONCLUSION:

In conclusion, digital health technology holds immense promise for transforming healthcare delivery, improving patient

outcomes, and enhancing the overall health and wellness of individuals. 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 challenges requires a holistic and collaborative effort involving healthcare professionals, technology developers, regulatory bodies, policymakers, 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.

ACKNOWLEDGMENT

All the authors are appreciated for their contribution and synthesis of the manuscript.

CONFLICT OF INTEREST

Authors declare no conflict of interest amongst themselves.

REFERNCES

[1] Sarbadhikari SN. The role of standards for digital health and health information management. J. Basic Clin. Res. (JBCR). 2019;6(1):1.

[2] https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health (Accessed on 27/07/2023)

[3] Voelker R. New center at FDA will advance digital health innovation. JAMA. 2020 Nov 3;324(17):1715-.

[4] Awad A, Trenfield SJ, Pollard TD, Ong JJ, Elbadawi M, McCoubrey LE, Goyanes A, Gaisford S, Basit AW. Connected healthcare: Improving patient care using digital health technologies. Advanced Drug Delivery Reviews. 2021 Nov 1;178:113958.

[5] 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 Jun 5;22(6):e17457.

[6] https://www.fda.gov/medical-devices/digital-health-center-excellence/guidances-digital-health-content (Accessed on 27/07/2023)

[7] Food and Drug Administration, 2019. Proposed regulatory framework for modifications to artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD)

[8] Dash S, Shakyawar SK, Sharma M, Kaushik S. Big data in healthcare: management, analysis and future prospects. Journal of big data. 2019 Dec;6(1):1-25.

[9] 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 (pp. 25-28). IOS Press.

[10] McHugh M, McCaffery F, Casey V. US FDA releases final rule on medical device data systems: what does this mean for device manufacturers.

[11] Yetisen AK, 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.

[12] Larson, D.B., Harvey, H., Rubin, D.L., Irani, N., Justin, R.T. and Langlotz, C.P., 2021. Regulatory frameworks for development and evaluation of artificial intelligence–based diagnostic imaging algorithms: summary and recommendations. *Journal of the American College of Radiology*, *18*(3), pp.413-424.

[13] Carroll N, Richardson I. Software-as-a-medical device: demystifying connected health regulations. Journal of Systems and Information Technology. 2016 May 9;18(2):186-215.

[14] Cheng M. Medical device regulations: global overview and guiding principles.

[15] Thapa C, Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine. 2021 Feb 1;129:104130.

[16] 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 Dec 10;6(4):e20579.

[17] Kinsel D. Design control requirements for medical device development. World Journal for Pediatric and Congenital Heart Surgery. 2012 Jan;3(1):77-81.

[18] Badnjević A, Pokvić LG, Deumic A, Becirovic LS. Post-market surveillance of medical devices: A review. Technology and Health Care. 2022(Preprint):1-5.