Emerging Digital Health Solutions: Inherent Challenges in the Technology Driven World

Posted 27 November 2019 | By Darin S. Oppenheimer, DRSc, FRAPS, RAC, PMP, George A. Cusatis MS, RAC, Suraj Ramachandran, MS, RAC, Jessica L. Hale, PharmD

This article explores the challenges of digital health solutions and emphasizes the appropriate controls necessary to help mitigate the risks and ensure companies are adhering to the growing needs of regulators and industry best practices.

Introduction

The opportunities and challenges in technology are driving explosive breakthroughs for digital health solutions in our technologically focused society. The accessibility, convenience and mobility of digital health has created a cultural shift in the way we utilize, process and provide healthcare solutions.¹ This transformational shift also has modified how one uses and obtains information from products and users in a real-world scenario, driving interest from many industries.

Pharmaceutical organizations, technology vendors and medical device organizations are creating digital health solutions for use in adherence, patient engagement, behavior management and companion solutions for treatment with existing products. While these advancements are continuously evolving, they share the common goal of assisting healthcare professionals, patients and data analysts with the ability to further advance diagnosis, treatment and provide a broader reach regarding education through the increased use in data and analytics.

However, using these types of products presents manufacturers with many unique risk management challenges that are typically embedded into the quality management systems of pharmaceutical and medical device organizations due to the inherent risks associated with these products regarding interoperability, cybersecurity and data privacy management.

Background

While global regulations continue to evolve to address these advancements in technology, one of the most significant changes is the legislative enactment of the 2016 21st Century Cures Act, which redefined what constitutes a medical device and clarified software applications which could be excluded.² While this seemed to increase transparency surrounding medical devices, digital health
solutions were omitted. This presented challenges for FDA’s regulatory oversight of software functions, as well as an organization’s compliance activities with postmarketing surveillance reporting requirements and expectations for best practices.

At a high level, if the intended use of the software function is related to the diagnosis, cure, mitigation, prevention or treatment of a disease or condition, the product falls within the definition of a medical device and thus becomes a regulated product. General wellness products help people manage their health and wellness, promote healthy living and gain access to useful information when and where they need it. However, due to the lack of significant risk involved, FDA has stated that regulatory oversight will not be applied to the general wellness products as the risk is minimal to the public.

Digital health incorporates technology and therapeutics to provide accessible tools such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth/telemedicine and personalized medicine. These are used by healthcare providers and others to reduce inefficiencies, improve access, reduce costs, increase quality and provide greater personalized therapeutics. Patients can use digital health technology to track and assist with managing disease states. A spectrum of intended use and expected outcomes exists due to the variety of end-users of the digital solution. This spectrum is further complicated by the increased accessibility of these products to the end-user and expanding consumer base, thus introducing risks which vary in type and impact to its end-user.

While it is understood that all products, especially those classified as medical devices have inherent risks, it cannot be overlooked that these digitally driven solutions may create a different approach to how we traditionally think about postmarketing activities and risk management for medical devices. Digital health solutions present a variety of unique challenges compared to traditional medical devices, drugs and biologics. The novel technology has unique attributes that need to be considered (e.g., cybersecurity). Drugs, biologics and medical devices have clearly defined classifications that describe the level of impact the event may or have had, which provides an appropriate path and subsequent actions forward for the healthcare provider. For example, medical device reporting is one of the postmarketing surveillance tools used to monitor device performance, detect potential safety issues and provide input for benefit-risk assessments of these products. According to 21 CFR 803, there are mandatory reporting requirements for manufacturers, importers and device user facilities and voluntary reporting from healthcare professionals, patients and consumers. Manufacturers and importers of medical devices are required to submit reports to FDA whenever they are aware of information which suggests that a marketed device may have directly caused or contributed to a patient’s serious injury and/or death. Often, patients will report any issues to the manufacturer rather than directly to FDA, so it is the manufacturer’s responsibility to convey such information to FDA.

Opportunities and Challenges

As we explore the challenges and opportunities of digital health solutions, we realize that one challenge that faces all manufactures is how to anticipate product failures that could pose safety risks for patients. This requirement becomes quite the challenge because the failures can have many different aspects contributing to them such as the product itself or through another product
interaction. These instances present unique challenges for manufacturers regarding interoperability, cybersecurity, data collection and privacy which will be discussed in greater detail.

**Device Interoperability**

Interoperability occurs when medical devices and digital solutions interact with one another. As interoperability becomes more prevalent, safety of the patient and operator is an important consideration. For example, a dosing calculator (digital solution) transmits weight in kg, but the receiving medical device assumes measurements in pounds. This can result in delivering the wrong dosing of a medication to a patient which could potentially result in serious injury and/or death. The challenge lies in determining which party is responsible for reporting the adverse event and where does the failure in communication occur. This specific example highlights the impact on reporting responsibilities and risk management challenges manufacturers are faced with. Appropriate safety considerations during initial device design can prevent unforeseen safety issues from occurring. Alignment between medical devices and digital solutions in the interoperability space is critical, especially on decisions regarding which party would be responsible for adverse event reporting.

Another risk common across all healthcare settings is the integrity of data management. If a digital product has a security breach and the product itself stores a patient’s information, this may enable access to the patient’s data. Security breaches not only introduce risks to the authenticity of data, but also puts the protection of their healthcare information at risk, as well as the patient’s safety. The interaction with multiple products regarding the interoperability opens pandoras box to numerous access points for inputs and further introduces room for error.

**Cybersecurity**

While digital health solutions present many challenges, there also are technological opportunities which should be examined, such as the potential to strengthen the safety and efficacy of digital health products. One promising addition to the future of digital health is the implementation of Artificial Intelligence and Machine Learning (AI/ML) as a supplement to bolster a product’s security. As AI becomes part of the industry’s common vernacular, we are discovering its benefits and how it may improve how information is processed for diagnosis and treatment. However, one area that is starting to gain momentum is how AI can be used in the area of embedded cybersecurity for digital health solutions.

AI is an application which can use different techniques enabling high-order functioning, such as continuous learning, which can have a significant impact in the realm of medical device cybersecurity. AI can collect real-time data with concurrent device usage, in which the software continues to learn through analyzing patterns of data. ML is one of the many techniques used to produce intelligent behavior, empowering the machine to not only learn from, but act upon the data captured. AI/ML can be used to design and train software algorithms to autonomously analyze the data to improve and optimize its performance to meet user-specific needs. Accordingly, with its unique, unprecedented capabilities, AI/ML-based Software as a Medical Device (SaMD) has the potential to provide a more robust level of cybersecurity; an innovative solution to traditional issues which are inherent to digital technologies. This would further compliment traditional risk management approaches, in addition to ensuring compliance with Good Machine Learning Practices (GMLP). This approach may be a
greater benefit in addition to traditional cybersecurity approaches such as dynamic passwords, penetration tests and simulated events used for traditional medical devices. Unlike traditional medical devices, these types of products may have multiple access points where security breaches can occur, which increases the risk of an event.

The same principle of artificial intelligence and machine learning in medical devices is also being used to increase efforts to secure patient data in the following four ways:9,10

1. Identify new malware threats with machine learning: predictive algorithms can learn to identify new threats and malware signatures to bridge the gap of protection from something that is unknown.
2. Identify and respond to breaches using behavioral modeling: AI can uncover and isolate anomalies within a network with continuous and automatic monitoring.
3. Protect medical devices from attack: AI can help avoid serious threats to patient safety by attacks that can influence or alter the performance of smart medical devices.
4. Extend human resources and address security shortages: AI solutions can supplement the IT security staff by providing continuous intelligent monitoring to avoid burnout of the staff.

Protection of Patient Data and Authenticity of Data
It is easy to understand the significant issues and risks of a security breach that involves healthcare data from a patient’s perspective, such as violation of privacy or identity theft, but there is an even greater risk to the healthcare industry. Healthcare information on the dark web can be used to buy medical equipment, drugs, or even fictitious claims with insurers. This creates a situation where medical information many times more than a patient’s financial information, such as a credit card.11,12

An important consideration, with the emergence of AI/ML-SaMD, is the need for real-world performance monitoring. This ensures that the SaMD is performing as intended, thus it is imperative that cybersecurity measures be included as a top objective during product development. Any compromise in cybersecurity could lead to significant impacts on the performance of the SaMD. Listed below are some potential outcomes with cybersecurity vulnerabilities:

- Patient data released to the public which can have profound impact with regard to patient privacy regulations.
- Healthcare providers or other critical stakeholders could be restricted from accessing information needed to perform an event to mitigate patient harm. Note: this output could be life-saving or life-sustaining.

Therefore, it is critical to incorporate cybersecurity measures during the ideation of digital health solutions to align with risk management and the quality system to incorporate these measures while in the design phase. By taking this approach, you inherently prioritize security measures as an objective in a quality management system approach as opposed to developing a product independently and incorporating cybersecurity measures after development has been completed.13-15
Best Practices for Industry

When laws and regulations are enacted, it is important to recognize that the regulations may not always solve the problem that spurred their enactment in the first place. This is where the importance of a thorough and well executed risk management and Quality Management System (QMS) are critical for a manufacturer. This ensures that the manufacturer of the digital health solution is continuously improving and monitoring the product and operations based on the feedback loops established to mitigate risk and continually learn. When incorporating digital health solutions into your organizational portfolio, it is important to understand that there are specific nuances for these types of products and they should be thought thoroughly how you want to ensure they are addressed in your organization’s QMS and its applicability to digital health solutions. The organization’s QMS should have procedures in place regarding the software design, development, validation, maintenance and performance monitoring to ensure a culture of robust quality and organizational excellence. Special consideration should be given throughout development, as well as improvement through change control, data management, evaluation and training. Business partners and third-party organizations for digital health solutions should embrace the same standards and controls for a robust system. This provides assurance that the organization produces or could produce, high-quality, safe and effective digital health solutions. Proper systems and controls should deliver and maintain high-quality products throughout the lifecycle and facilitate marketing submission for a new digital health product.

Conclusion

As digital health solutions continue to become more prevalent in our society, it is essential for manufacturers to have appropriate risk mitigation measures and controls in place allowing for robust risk mitigation. Manufacturers should design their process of collecting clinical evidence with the patient in mind, imposing the least burdensome approach, as well as considering the appropriate level of patient de-identification and determining what information is necessary to assess performance and quality, as well as the intended use through patient outcomes. Education should be provided to end-users regarding how their personal information will be used and what information to omit and the potential risks associated. The more unnecessary data that is captured, the greater the risk, resulting in misuse of the patient’s health data leading to a perpetuating cycle of technology avoidance and missed opportunities for advancing healthcare.

References


**About the Authors**

**Darin S. Oppenheimer, DRSc, FRAPS, RAC, PMP,** is executive director of the Device and Digital Health Group, focusing on Medical Devices and Combination Products at Merck, based in Upper Gwynedd, PA. He joined Merck with 16 years of experience in many facets of the product development lifecycle, including regulatory submissions and due diligence. He has actively participated with industry trade organizations and on standards committees. His time as a research and development scientist focused on pharmaceuticals and medical device diagnostic applications for biomarker and drug discovery. His educational background includes two master degrees from Johns Hopkins University in biotechnology and regulatory science and a graduate certificate in biotechnology enterprise also from JHU. He completed his DRSc in regulatory science from the University of Southern California in 2016. He is a 2017 RAPS Fellow, serves on the Editorial Advisory Committee for RAPS *Regulatory Focus* and the Editorial Board of the Institute of Validation Technology. He can be contacted at darin.oppenheimer@merck.com.

**George A. Cusatis, MS, RAC,** is associate director of Merck’s Device and Digital Health Group, based in Upper Gwynedd, PA. In this role, he supports the Medical Device and Combination Product (MDCP) and digital health solutions business across Merck. Cusatis provides guidance and support for more than 40 products, including auto injectors, prefilled syringes, digital health software and contraceptives. He has extensive experience with the product development lifecycle, including product safety, regulatory submissions, quality assurance and clinical affairs. Custis received a MS in regulatory affairs/quality assurance from Temple University and a MS in bioengineering from Syracuse University. He is a member of the RAPS, ASQ and DIA professional societies and holds ISO
certifications in Quality Management Systems Requirements (ISO 9001), Information Security Management (ISO 27001) and Medical Devices Quality Management Systems (ISO 13485). He can be contacted at george.cusatis@merck.com.

**Suraj Ramachandran, MS, RAC**, is a director, regulatory affairs in the Device and Digital Health Group at Merck based in Rahway, NJ. Ramachandran is currently responsible for supporting various medical devices and combination products, such as auto injectors, prefilled syringes, inhalers and contraceptives. In addition, he is heavily involved in providing guidance for digital solutions and has led many development efforts regarding medical device software, intended for both domestic and international markets. In previous roles within industry, he was responsible for an infusion pump platform as well as supporting all new product development and lifecycle maintenance activities including regulatory submissions, design control, audits and CAPAs. Ramachandran holds a master’s degree in biomedical engineering from the University of Michigan. In addition, he has earned the RAPS RAC. He can be contacted at suraj.ramachandran@merck.com.

**Jessica L. Hale, PharmD**, is a senior specialist in the Device and Digital Health Group at Merck based in Rahway, NJ. Hale joined Merck as a regulatory affairs intern while entering her third year of Pharmacy School, with prior pharmacy experience in both the hospital and community settings in addition to conducting pharmaceutical formulation research. Combining her passion for patient care with her curiosity and analytical mindset, Hale has continued her role within regulatory affairs, working to optimize patients access to therapies. She received her Doctor of Pharmacy degree in May 2019. She can be contacted at jessica.hale@merck.com.