



WHITEPAPER

The Rapid Rise of Digital Health Technology: Challenges and Keys to Success



Written in conjunction
with Beanstock Ventures

What is Digital Health?

Digital health merges digital technologies with health, healthcare, living, and society to enhance the efficiency of healthcare delivery to make medicine more personalized and precise.

Digital health is a broad category that includes:

- Mobile health (mHealth)
- Health information technology (IT)
- Wearable devices
- Telehealth
- Telemedicine
- Personalized medicine

Digital health technologies use:

- Computing platforms
- Connectivity
- Software
- Sensors

These technologies are intended for use as a medical product, as companion diagnostics, or as an adjunct to other medical products.

Digital Health vs. SaMD: What's the difference?

Digital Health

Uses computing platforms, connectivity, software and sensors for health care and related uses. These technologies span a wide range of uses, from applications in general wellness to applications as a medical device.

SaMD

A subset of digital health, software that performs one or more medical functions. While the software may be embedded in a piece of hardware (as is often the case), it's the software itself that performs the medical function.

The Rise of Digital Health

The past decade has ushered in major disruption in all industries, including the medical device and life science sectors. Market disruptors such as smartphones, social media, and more transformed the way that people work, play, and manage their health. Software has transformed how doctors practice medicine, how people manage their health, and the fundamental interactions between patients and providers. During this process, the boundaries between digital health and medical devices began to blur.

According to the Federal Drug Administration (FDA), “Digital health technologies use computing platforms, connectivity, software, and sensors for healthcare and related uses. These technologies span a wide range of uses, from applications in general wellness to applications as a medical device.” These applications are driving a lot of the wearables we see today, like a heart rate monitor running on a smart watch or a mobile application connected to a wearable. Other examples of digital health applications might be something like 23andMe, which uses genetic sequencing data to identify health risk factors.



The Emergence of Software as a Medical Device (SaMD)

Traditionally medical devices have been classified as an instrument, sometimes with software running on the actual device itself.

The lines between digital health technology and medical devices get crossed once the software technology begins to perform a medical function, especially if the technology is not embedded within the medical device. Consider software that determines the right medicine dose for a patient based on his or her personal data, or software that detects and diagnoses a stroke through analyzing MRI images. These are examples of software that could be serving as a medical device.


As digital health has pushed further and further into the traditional realm of medical devices, an entirely new category was formed and regulated, which is software as a medical device (known as “SaMD”). SaMD is described as “software that performs one or more medical functions. While the software may be embedded in a piece of hardware (as is often the case), it’s the software itself that performs the medical function.”

With the emergence of software as a medical device, there are questions around risks, regulations and safety. Understanding trends and potential risks can help teams mitigate challenges and navigate forward with greater success.

The Digital Health Market: Potential Challenges and Recommendations to Address Them

The digital health market is full of potential pitfalls that can delay or even stop your product from coming to market. If you understand where the challenges typically reside, you can more effectively anticipate their presence, mitigate them, and develop a more proactive strategy towards product development. Consider the following.

- **Risk management.** If you look at traditional medical devices, the way that medical device manufacturers often managed cybersecurity and data privacy risks was by controlling and limiting the availability and accessibility of protected health information (PHI). Embedded medical devices can be completely locked down and isolated from the rest of the healthcare eco-system. Smartphones and newer digital technologies, however, are highly integrated within the healthcare eco-system, where data availability and accessibility are essential to their core operation. Take for example a diabetic patient who relies on a glucose monitor application running on his or her smartphone sending data to and from a wireless enabled wearable glucose monitor.



RECOMMENDATION: It is important to understand the risks associated with transmitting protected health information wirelessly and then implementing and validating proper risk controls measures to ensure the data is protected and can be relied upon.

- **Data privacy.** Data privacy breaches of protected health information is a major area of concern in today's highly integrated environment. New laws are continually emerging focused on maintaining data privacy and protecting sensitive health care data which impact both the medical device manufacture and the healthcare provider who manage health care data.

RECOMMENDATION: Integrate data privacy considerations into your risk management and software development process at product inception, and as part of your architectural design.

- **Cybersecurity.** Threats and vulnerabilities are something all developers need to mitigate with their digital health solutions. Manufacturers, hospitals, and facilities all need to work together to manage cybersecurity risks.

RECOMMENDATION: Architect and design your product with cybersecurity in mind and gain a detailed understanding of cybersecurity upfront and understand where the vulnerabilities lie withing your product design. Also consider consulting with cybersecurity experts as needed.

- **Interoperability.** Another potential pitfall is not designing your software as a medical device for interoperability. The current healthcare ecosystem in which many digital health applications are reliant upon is complex and vast. Despite the creation of messaging standards such as FHIR, DICOM and HL7, the adoption has been slow, and the use of these standards has been inconsistent.

RECOMMENDATION: Consider where your software as a medical device product will be deployed and how it will be integrated into the various parts of the health eco-system (EMR, medical devices, LIMs, Patient Portals, etc.). For complex environments, focus on a few key vendors that support your initial product launch and ensure you understand and can mitigate the potential risks associated with integrating into third-party vendor applications.

Keys to Success in the Digital Health Medical Device Market

Meeting regulations is complex. Initially, there were a few guidance documents and regulations related to medical device software, but with the advancement of the internet and the cloud, regulations have expanded to cover digital health, cybersecurity, AI, etc.

The challenge is how do you integrate guidance and regulations into your existing quality management system and software development process?

You might be asking yourself, “Where do we even start?”

The key for companies embarking on these new digital health solutions and getting them to market is to avoid overthinking the regulations and go back to good software engineering practices.

Companies that are not overly familiar with software-specific regulations and guidance often create overly complex and burdensome processes because they lack an understanding of the true intent of the regulations and guidance documents. If you're spending 80% of your time doing documentation and 20% doing design development and testing, then you're missing the mark.

Instead, spend time understanding the intent of the regulations and how your current software development practices can apply and resist the urge to “over-proceduralize” them.

The good news is, if your team members are well trained and educated, they are likely already following best practices.

In addition to your current software development practices, consider the following practices to reduce risk and ease the path to compliance:

Managing risk throughout the development process

Ideally, you're performing risk management throughout the end-to-end development process. You're doing it upfront with your risk management plan, you're making sure that it's built into the development, it's factored into the requirements, you're doing a proper hazard analysis, you're even looking at hazards as it relates to overall verification and defects that come out of the testing.

Focus on components and processes in design history file creation

Create Design History Files (DHF) that focus on components and processes. Understand how your software will interface with the entire ecosystem while meeting patients' and users' needs. Decompose your system, plan, and conduct your design activities and create design deliverables to manage risks. This encompasses planning documentation, system architecture, risk management, and more.

Highlight key integrations

Use tools to facilitate compliance. Include key integrations such as design control systems, document control systems, LMS training systems, defect management, and risk management. Also, integrate post-market surveillance into software development lifecycle management by getting feedback looped into product engagement and design changes.

Detail cybersecurity considerations

Design against cybersecurity issues and understand cybersecurity upfront. Focus on cybersecurity, such as designing against potential threats and integrating safeguards into your software development lifecycle. Cybersecurity should be carefully woven throughout the ecosystem. Understand what platforms are involved within the ecosystems and how they will interface with the medical device software.

From an architectural perspective, think about cybersecurity concerns at the interface level and where you're exposed. And then from a design perspective, how am I going to implement some of the cybersecurity measures just like you would for your risk mitigations as well.

Collaborate across all vendors

Lean on vendors to help meet compliance requirements. Google, Microsoft, Amazon, and others offer disclosure statements that can support compliance with specific regulations, such as GDPR. In some cases, it can be more reliable and efficient to rely on the ecosystem of large players rather than outsourcing the development to create your own custom solutions.



How Requirements Management (RM) Software Can Support Best Practices

Stay proactive during the development of your product or system and adopt a modern requirements management solution, which allows development teams to focus on these six key areas:

Understand visibility across development

Digital health development isn't just about software teams – marketing, product, software, quality, and other teams need to stay up to date in real time.

Too often teams rely on paper based or manual systems to manage requirements, which can introduce risk into the process. A closed-loop requirements management solution can provide full visibility across all development activities and detailed traceability, from the high-level user needs through to validation and verification.

With digital health design controls implemented in a requirements management all stakeholders involved with the development process can understand progress, dependencies, and their impact and ultimately know who to collaborate with at different design stages.

Maintain end-to-end traceability with closed-loop requirements management

Traceability ensures that regulation and product requirements have been met and verified, providing necessary evidence from the design control process to the regulators. Traceability of data to data and traceability of the people connected to that data help teams analyze the who, what, where, and why of each requirement to ensure that essential information doesn't get missed.

A requirements tool that enables real-time bi-directional traceability in a centralized location is key to ensuring that all development activities have been addressed, with no gaps. Additionally, a tool which enables stakeholder collaboration across linked activities is a must have, allowing cross functional teams to easily understand why decisions were made.

Release and configuration management

A modern requirements management solution can support different scenarios that can help with your configuration management and versioning of systems. You can quickly build standard libraries and reuse core requirements, risks, tests, and other development artifacts. Whether you deploy linear or parallel release management methodologies, teams can quickly understand release scope, produce relevant documentation, and push and pull changes across different versions.

Change management

21 CFR 820.30 and ISO 13485 discuss the need for a robust and well-established change management process. Implement a requirements management tool that will support change management through the maintenance of version history, document control (as defined by the FDA in 1997 as “all design documents, drawing, and other items of design input or output which characterize the design or some aspect of it,” traceability to a change request, and access to a clearly defined line of impact via a trace matrix or comparison view report. A review and approval process embedded in the requirements management tool will allow stakeholders to understand the scope and impact of the change quickly and accurately prior to making such change.

Verification and validation

Requirements must be verified to have been implemented correctly, and user needs must be validated to ensure that the product satisfies the user’s need and that the right product was built for the customer. Validation activities include human factors testing, clinical evaluation to determine the efficacy of the software for its intended use, or a demonstration to ensure that risk controls are effective. This requires more than just your standard set of software testing, which typically consists of code reviews, unit testing, static analysis, integration testing, and requirements-based testing.

A tool that enables capturing the results of V & V activities, with links to requirements is a must have to clearly visualize that the product is functioning and performing as expected. The ability to trace failed tests to new and existing defects for quick resolution is also critical, enabling a centralized view of end-to-end development, from high level user needs, down to granular defects.

Perform risk management early

Many digital health companies continue to depend on spreadsheets to capture risk data. Connecting that information back to design controls is a cumbersome and error-prone process. Static documents, like spreadsheets don’t allow for automated traceability, so risks and requirements don’t live in the same system. This makes it tedious and time-consuming to conclusively demonstrate compliance.

Capturing risk analysis directly in a requirements management solution allows team to build risk management into the development process and requirements and tests are connected to risk and hazard analysis.



How Beanstalk Ventures Can Help

BeanStock Ventures is a project-based Software Development and Regulatory services with expertise in Digital Health including regulatory expertise in SaMD and Cybersecurity. With over 20 years of regulatory and software development experience, BeanStock Ventures has healthcare specific domains including but not limited to embedded devices, biotechnology, diagnostics, IoMT, the point of care, critical care, laboratory, automation, analytic, workflows, and connectivity.

The BeanStock Ventures service offerings include technical program management, software product development and regulatory compliance. In addition to the BeanStock Ventures domain expertise and experience in the medical device, biotechnology, and life sciences industry, it is also one of nine companies globally that has been approved as an FDA-Accredited 510(k) Third-Party Reviewer for the United States Food and Drug Administration (FDA).

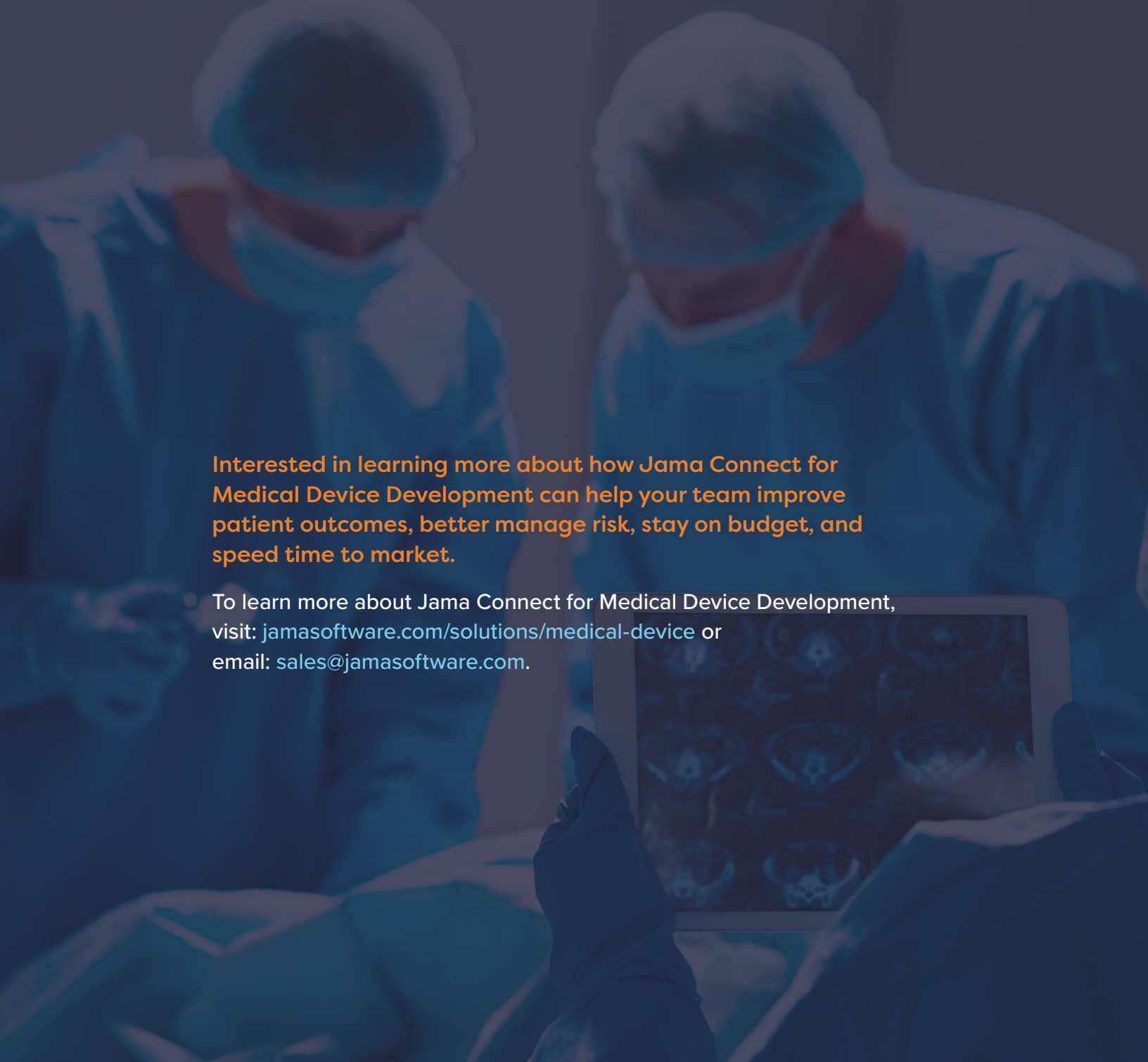
For more information, please visit: www.beanstockventures.com or email marketing@beanstockventures.com.

How Jama Software Can Help

For medical software manufacturers, compliance is an important goal, but it is not the only factor when delivering safe and reliable products to market. To achieve compliance, organizations need defined processes for development and production and closed-loop requirements management, from the high-level user needs through to validation and verification.

Focus and rigor in the systems development lifecycle drives compliance as an outcome. Jama Connect® for Digital Health eases the path to compliance so companies can focus on systems development, spending less time on paperwork and more time on innovation.

Customers trust Jama Connect to streamline their systems development with design control templates aligned with industry standards, compliant reviews and approvals, and end-to-end traceability, making audit preparation and record-keeping a straightforward process.



Interested in learning more about how **Jama Connect for Medical Device Development** can help your team improve patient outcomes, better manage risk, stay on budget, and speed time to market.

- To learn more about **Jama Connect for Medical Device Development**, visit: jamasoftware.com/solutions/medical-device or email: sales@jamasoftware.com.



ABOUT JAMA SOFTWARE

Jama Software is focused on maximizing innovation success. Numerous firsts for humanity in fields such as fuel cells, electrification, space, autonomous vehicles, surgical robotics, and more all rely on **Jama Connect®** to minimize the risk of product failure, delays, cost overruns, compliance gaps, defects, and rework. **Jama Connect®** uniquely creates **Living Requirements™** that form the digital thread through siloed development, test and risk activities to provide end-to-end compliance, risk mitigation, and process improvement. Our rapidly growing customer base of more than 12.5 million users across 30 countries spans the automotive, medical device, life sciences, semiconductor, aerospace & defense, industrial manufacturing, financial services, and insurance industries. To learn more, please visit us at jamasoftware.com.