Dynamic Blog

5 Challenges with Medical Device Technologies and How to Solve Them

There has never been a more crucial need for medical devices than today. With the power to sustain and improve the lives of so many people, it's critical to ensure these devices are secure, effective and high quality, especially the technology that enables them to perform processes and operations of the utmost importance. From ventilators to smart medication dispensers, real-time health systems, ingestible sensors and more, medical devices are highly regulated and scrutinized for errors — which no manufacturer can afford to make. Find out some of the top challenges that can accompany medical device technology as well as potential solutions.

1. Developing a Comprehensive Understanding of End Users

The basis of creating successful medical devices is having a clear view of the people who will be on the receiving end of the products and accompanying technology. From patients to physicians and home caregivers, end users must be able to comprehend how to operate devices, the same way manufacturers must be able to communicate the purpose and value behind the products. To solve for this issue, medical device manufacturers can establish closer relationships with the patients, physicians and healthcare leaders that use their products, as well as devise new business models that rely on a broader range of inputs — incorporating an end-to-end documentation strategy for product development which includes extensive real-world data and usability feedback. All of this can help meet end-user demands such as more personalization and simpler procedures, all while satisfying regulatory obligations and safety requirements.

2. Prioritizing and Ramping Up Cybersecurity

According to The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), data breaches in healthcare increased from 2018 to 2019 by 196 percent. Additionally, nearly 70 percent of medical device manufacturers say an attack on their equipment is likely, but just 17 percent of those companies are actively trying to stop these attacks. Cybersecurity is one area of product management that manufacturers can't neglect, as the protection of these devices is a life or death situation. There have been past instances of pacemakers, insulin pumps and surgical robots all being hacked. The solution to ensuring medical devices are protected from cyberattacks is to start thinking about it at the very beginning of product development, with engineering teams utilizing a "security-by-design" approach and building security directly into devices — as opposed to adding on security tools later, past the product delivery and deployment stages. This ensures security beyond traditional firewalls and also provides the ability to customize protection for individual devices.

3. Meeting Compliance and Regulatory Requirements

Per the U.S. Food and Drug Administration, medical device manufacturers are responsible for developing quality systems for each type or family of devices, adhering to all specs and regulations for safety and efficiency. Known as Current Good Manufacturing Practices (CGMPs), this quality system plays a vital part in any supply chain for medical devices. Additionally, under the Medical Device Reporting (MDR) regulation, manufacturers are held accountable for reporting specific adverse events or problems with their medical devices to the FDA. One of the hang-ups that corresponds with this is the complexity of such regulatory requirements, which can pose a roadblock and slow device availability to the public; on the other hand, these same regulatory requirements are sometimes not strong enough, which can then put people at risk. A potential solution for this is focused on collaboration among medical device manufacturers, pharmaceuticals, hospitals and other health facilities — working together closely to navigate regulations and mitigate risks throughout quality control processes and product lifecycles. Communicating necessary changes to devices, such as network upgrades or new patches, is also a joint responsibility of both manufacturers and healthcare organizations.

4. Focusing on Interoperability

The Healthcare Information and Management Systems (HIMSS) defines interoperability as "the ability of different information systems, devices and applications ('systems') to access, exchange, integrate and cooperatively use data in a coordinated manner, within and across organizational, regional and national boundaries, to provide timely and seamless portability of information and optimize the health of individuals and populations globally." Interoperability can pose a challenge in a couple of ways. First, information sharing often comes with privacy and security risks, and there is not much of an incentive for stakeholders in the private sector to push for interoperability efforts. Second, limitations in vendors' healthcare technology offerings make it tough to copy or share information from one type of electronic health record software or technology to another. This wide range of complex processes, clinical standards and diverse vendors can make it difficult to provide efficient patient care outcomes. This can be solved if healthcare and tech providers collaborate on developing a set of standards for interoperability — as well as a unified, open platform including health data exchange architectures and application interfaces — to share clinical data and messaging.

5. Securing Trust in Medical Technology

Medical devices can typically only succeed and deliver their designated outcomes if patients are willing to share their health data. Lack of transparency about where data will be used and stored, as well as who will have access to it, is one of the primary reasons patients fail to trust healthcare providers and organizations with their personal information. In the digital age, securing patient trust means that healthcare organizations need to take a data-centric security approach; this means increasing data privacy measures such as data encryption and authentication, as well as potentially using embedded blockchain-like technology to offer real-time mechanisms and insights into how data is processed. Giving patients control over their own data, enabling them to view the purposes and users of their data, can also serve as an avenue for increasing patient trust.

Mission-critical equipment like medical devices and their accompanying technological components serves such an essential purpose in the world today. Being cognizant of some of the primary challenges facing medical device manufacturers today is paramount to developing a proactive strategy, securing patient data and trust while delivering products that achieve their designated outcome of bettering the lives of humans.

Have Questions?

Dynamic offers a digital management platform for data collection and analysis, as well as IoT product development, for all your connected medical devices. Contact us at 866-399-1084 or info@dccit.com to find out more.

Rachel Zachar
Content Manager

Search

CATEGORIES

Technology Supply Chain Management
Validation & Testing Solutions
Complex Technical Configuration
Technology Asset Lifecycle Management
Thought Leadership
Company News
Uncategorized

SUBSCRIBE TO OUR POSTS

Email*

Subscribe

RECENT POSTS

Just-In-Time Inventory Management May No Longer Be Viable. What's Your Strategy Now?
June 14, 2021

Managing the Lifecycles of Medical Device Workstations
June 2, 2021

Dynamic Computer Corporation Changes Brand Name; Will Operate as Dynamic Technology Solutions℠
May 13, 2021