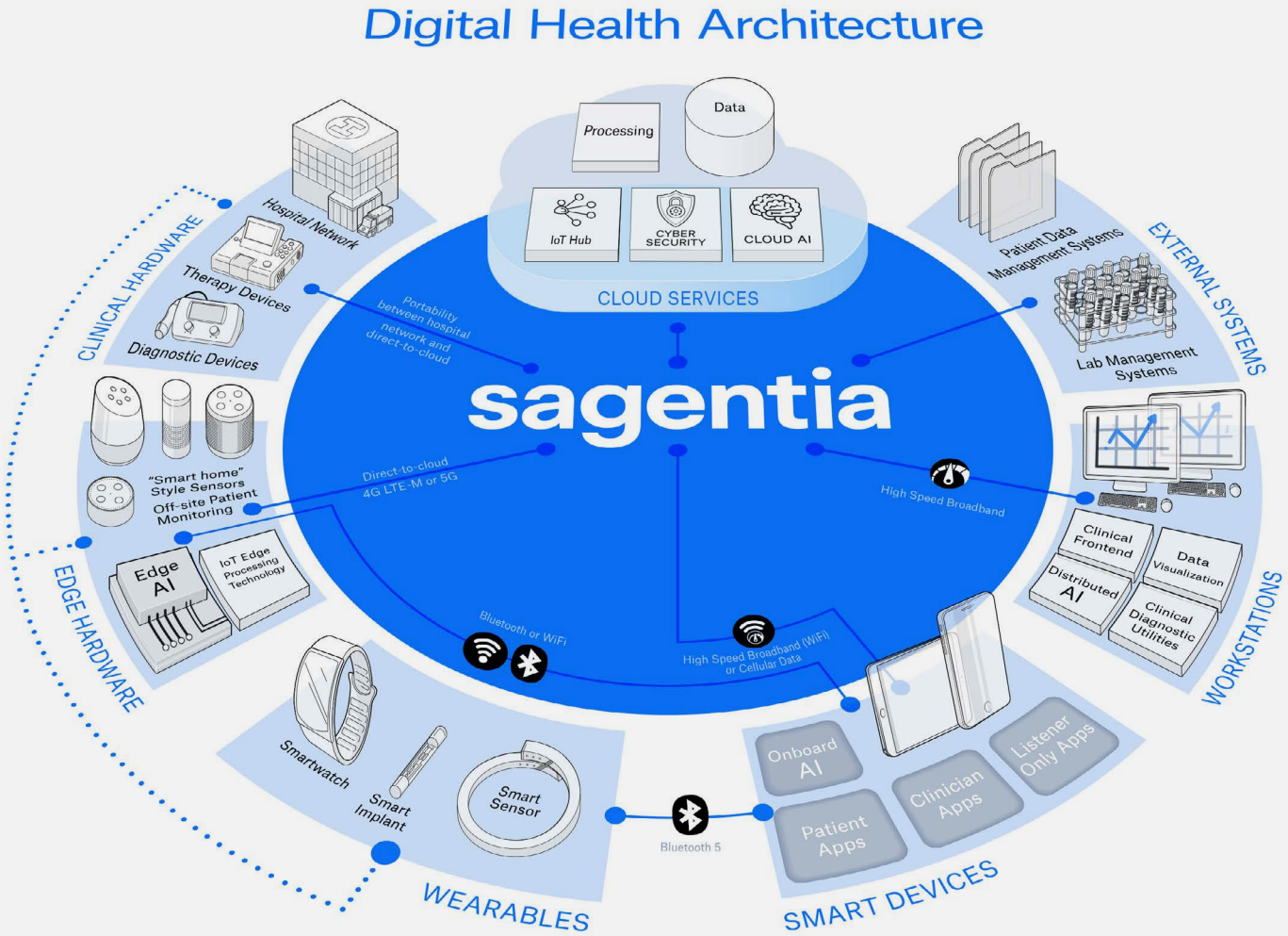
sagentia

Critical success factors for Medical IoT and Direct-to-Cloud devices

By Mat Spenger



Sophisticated cloud-based architectures unlock new possibilities for innovative digital platforms that improve patient outcomes efficiently and cost effectively. With the right blend of expertise and insight, off the shelf platforms can be integrated to deliver healthcare solutions that meet stringent regulatory requirements.

Our Architecting Digital Health Platforms series explores core segments of this dynamic environment. We unravel the complexity and identify issues device manufacturers may need to overcome to gain competitive edge. Here, we look at ways to leverage connectivity and direct-to-cloud capabilities and earn a slice of the burgeoning digital healthcare market.

sagentia

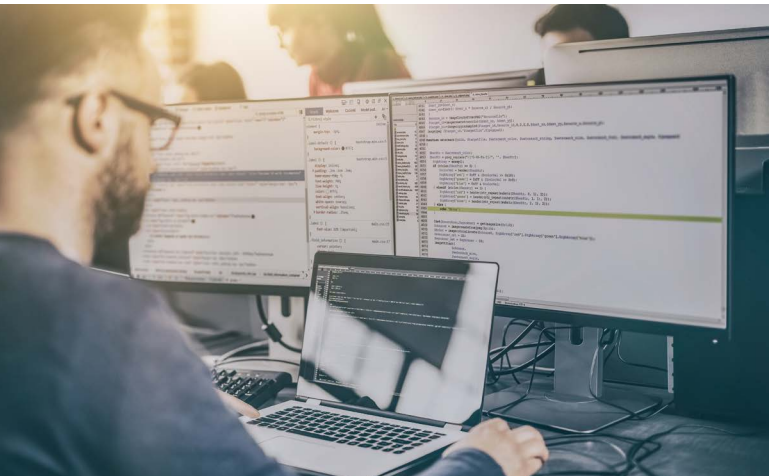
Digital devices have become commonplace in consumer health applications, as evidenced by the assimilation of fitness and wellness trackers. The possibilities to extend this to medical-grade devices are vast and manufacturers have a golden opportunity to innovate and gain market share. However, new products and solutions need to overcome different challenges to achieve traction in the medical-grade world.

On the face of it, Platform as a Service (PaaS) offerings from leading cloud providers make it easier than ever to create and iterate products quickly. But manufacturers need to be mindful of regulatory requirements as well as the safety and security of users and patients.

Collaborating with specialist medical device software architects can help avoid the conundrum of 'not knowing what you don't know'. Embracing this knowledge and insight at an early stage in the product development cycle can avoid costly and time-consuming issues further down the line, which may impact usability and uptake or even prevent FDA approval.

In this paper, one of our software consultants, Mat Spenger, looks at important considerations related to two key areas of the digital health market:

- Medical Internet of Things (IoT) devices that connect with each other or central hosts via a global network
- Direct-to-Cloud (D2C) devices which can communicate with remote hosts directly without a wired network connection, for instance using mobile data.



Platform

The top three cloud providers, AWS, Azure and Google Cloud, all offer powerful toolkits to aid the management of Medical IoT networks. Authentication and monitoring of devices and their traffic is relatively straightforward. Diagnostics and data management can also be supported to some extent with standard tooling. Where standard tools fall short, it's possible to link up with other cloud managed products, for instance to enhance processing power or data and diagnostic capabilities.

However, selecting the most appropriate tools and components, then integrating them in the most effective way, demands both technical expertise and sector insight. The requirements of a D2C asthma inhaler that conveys usage frequency to a remote host might be quite different from those of a smart device tracking patients' mobility levels following hip surgery.

It's important to focus on device objectives and wider factors such as use case, patient specification and use environment upfront. Each of these may have associated repercussions related to safety, regulations and ease of use which could be impacted by early decisions concerning platform architecture and tools. This is also the time to proactively consider the merits of vendor-specific versus vendor agnostic features, as well as ongoing requirements such as feature upgrades, and how those will be rolled out to remote devices.

Network

When it comes to D2C enabled devices, there are significant implications for product design and digital architecture. The nature and extent of these varies depending on the likely use case, use environment and user demands of the end product. All these factors have a bearing on the choice of device hardware.

A key challenge is disparities in networks, both internationally and regionally. While virtual SIMs can eradicate the need for multiple SIM cards if a patient is travelling, coverage of 5G and 4G LTE-M remains patchy. Ideally D2C devices should be able to function on older technology as well as taking advantage of emerging networks. If they cannot connect or operate in certain circumstances, it should be made very clear to the user that this is the case.

The costs and fair use limits of individual networks also need to be factored in, both to maximise uninterrupted service and ensure the whole lifecycle cost of the product is understood. Core requirements, such as an ability to transition between clinic networks and D2C, need to be fully mapped out, as these capabilities impact the required hardware complexity.

Ultimately, manufacturers need to understand where the challenges lie, in terms of patient, treatment environment and the network itself. This enables solutions to be architected in a way that addresses such issues to meet treatment objectives as seamlessly as possible.

Security & compliance measures

It's more than a decade since doctors replacing Vice President Dick Cheney's heart defibrillator modified it to prevent hacking risks. But the case underlines vulnerabilities that still exist in digital healthcare today. In 2017, the FDA recalled half a million pacemakers amid fears that they could be compromised by cybercriminals.

Minimising the potential for harm in the event of cybersecurity incidents needs to be front of mind in the design and development of devices and system architectures alike. Robust security protocols are vital. During the design phase, the primary focus is identifying potential threats and vulnerabilities, then assessing their potential impact on device functionality and the wellbeing of patients and users.

Addressing this at an early stage in the process results in more robust and efficient mitigation of patient or user risk. FDA guidance for the cybersecurity of medical devices should inform the entire product development process. Robust documentation is required to gain FDA approval, including detailed hazard analysis, a traceability matrix, plans for updates and security patches, malware controls and specifications related to cybersecurity controls such as antivirus software.

Gaining competitive edge in future digital health

The next decade will see significant changes in global healthcare systems. There's a pressing need to achieve better patient outcomes while keeping costs stable. With growing and ageing populations, that means actively reducing costs per capita.

Digital technologies offer much potential to achieve this goal, with Medical IoT and D2C devices set to play an integral role boosting treatment efficiency and effectiveness.

Device manufacturers need to drive focused innovations for specific medical contexts and applications, within the parameters of regulatory frameworks.

Those taking an holistic, well-informed approach will accelerate the journey from concept to launch, enabling them to thrive in the rapidly evolving age of digital health.

About Sagentia

Sagentia is a global science, product and technology development company. Our mission is to help companies maximize the value of their investments in R&D. We partner with clients in the medical, consumer, industrial and food & beverage sectors to help them understand the technology and market landscape, decide their future strategy, solve the complex science and technology challenges and deliver commercially successful products.

Sagentia employs over 150 scientists, engineers and market experts and is a Science Group company. Science Group provides independent advisory and leading-edge product development services focused on science and technology initiatives. It has ten offices globally, two UK-based dedicated R&D innovation centers and more than 350 employees. Other Science Group companies include OTM Consulting, Oakland Innovation, Leatherhead Food Research and TSG Consulting.

For further information visit us at:

www.sagentia.com
or email info@sagentia.com
www.sciencegroup.com

sagentia

Sagentia Ltd
Harston Mill
Harston
Cambridge
CB22 7GG
UK

Sagentia Ltd
First Floor
17 Waterloo Place
London
SW1Y 4AR
UK

Sagentia Inc
One Beacon Street
15th floor, Suite 1500
Boston
MA 02108
USA