SKYDATA-IoT

Transforming Lives with Real-Time Health Data

Connected healthcare plays a critical life-saving role in patient care and research. Healthcare professionals using telehealth applications should not need to worry about device connectivity in mission-critical situations, nor should researchers conducting clinical outcome assessments (COAs).

Maintaining stable device connections and data security in mobile health scenarios can be challenging. Many smart healthcare devices, such as monitors and trackers, rely on Wi-Fi or Bluetooth alone to send and receive data which need to be within range of a cellular phone, internet router, or gateway to connect to the cloud and transmit their data, often in lag time vs. real-time data.

In remote healthcare settings, Wi-Fi and Bluetooth wireless technology might not be enough to provide real-time connectivity. As cellular IoT coverage becomes ubiquitous worldwide, Healthcare Providers are considering it a viable add-on and/or alternative to connect their medical IoT devices.

This article will explore the benefits of a integrated approach to connectivity in remote or mobile healthcare settings.

Limitations of Using Wi-Fi and/or Bluetooth Technology alone for Connected Healthcare

Wi-Fi is a cost-effective solution suitable for many situations but has several drawbacks when used alone, including potential security challenges and coverage limitations. Wi-Fi relies on an intermediary transmitter—the router to deliver connectivity to end devices. Wi-Fi routers provide strong signals within a limited area around the network they create; however, the network's footprint is restricted regarding widespread coverage.

Bluetooth technology can reach up to 100 meters outdoors under optimal conditions. Recent advancements in Bluetooth Low Energy 5.0 technology offer extended ranges with lower power consumption. Similar to Wi-Fi, Bluetooth technology depends on a local hub to establish and maintain connectivity (e.g., pairing an end device with a smartphone).

Sections

Advantages of Integrating Cellular IoT Connectivity for Smart Healthcare

Reliability

In order to be effective, it is necessary for any medical device to maintain stable connections across different locations. For example, if a healthcare worker visits an elderly patient's home and the worker's devices rely on Wi-Fi, but the patient lacks a broadband connection or do not meet security credentials, the device may be unable to add/receive/analyze data to provide directly observed patient care.

Devices with Bluetooth technology also require pairing with a smartphone or other gateway device. When combined with a cellular solution it enables telehealth end devices to stay online without an intermediary, even while traveling out of range.

Scalability

Wi-Fi access points could limit the number of devices that can simultaneously connect. Supporting more devices requires installing additional Wi-Fi equipment, which may work well in specific scenarios like dedicated facilities. However, healthcare providers may need to deploy numerous medical IoT devices at once. Cellular provides scalability without extensive infrastructure adjustments. While there are scaling limits with cellular, they are significantly higher. Moreover, cellular infrastructure contains substantial intelligence to handle peaks in demand.

Enhanced Data Accessibility

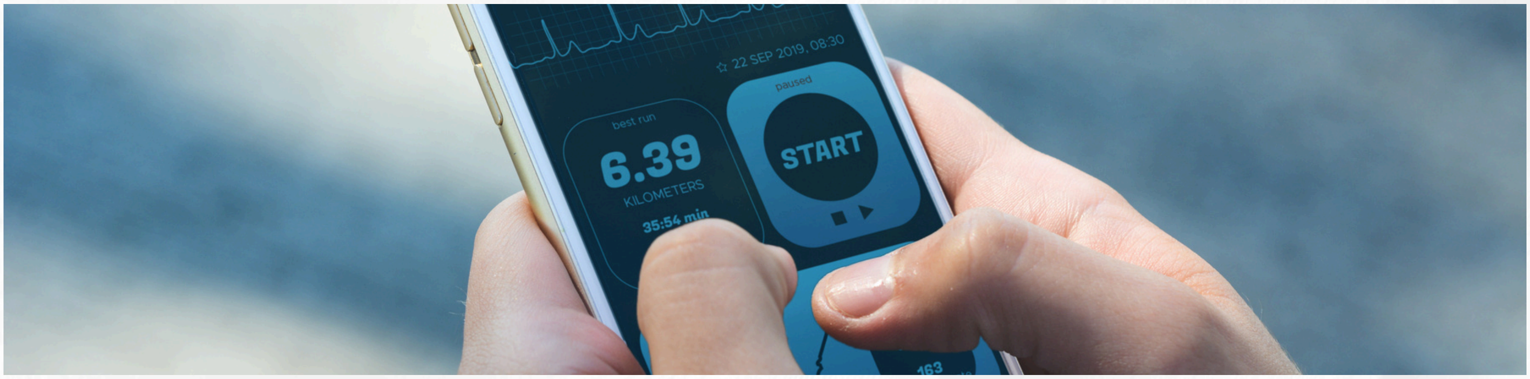
Healthcare providers require access to anonymized patient data to optimize analytics. Such data can generate risk scores, and identify variables in test results leading to improved patient outcomes.

Wearable sensors for certain conditions, offer objective measures of gait, balance, and physical activity, providing valuable insights into patient behavior and response to treatment during both active tasks and passive monitoring.

Collecting patient data efficiently can be challenging within a Wi-Fi or Bluetooth infrastructure alone due to firewall restrictions. When combined with cellular connectivity, researchers get to access anonymized data sets effectively while ensuring security and privacy.

Security

Wi-Fi networks must be actively protected from cybersecurity breaches. Although Wi-Fi networks feature encryption capabilities, these only function when enabled. New threats continuously emerge, requiring network managers to update security patches regularly. In contrast, cellular data encryption is the default setting, and the provider's cybersecurity team manages security updates. While Wi-Fi 6 introduces new security features with WPA3, cellular networks inherently offer more robust end-to-end security.



Assessing Your Smart Healthcare Device's Connectivity Needs

There is no universal connectivity option for connected healthcare devices. OEMs must evaluate their case needs to determine the best solution. Key questions include:

- In which regions will the device be deployed? What regulations regarding data ownership, privacy and security must be followed?
- Is the device mainly fixed or mobile? Will it be used while traveling?
- How much data will the device consume? Does it handle high-definition video or images, medical data, or real-time voice communications?
- Will multiple devices connect simultaneously, such as in a hospital setting?
- Can the device rely on the patient's home internet connection if it uses Wi-Fi?
- How will connectivity type impact device aesthetics, such as antennas?
- Are location services needed?
- What are the hardware requirements

Drop-In Networking

Cellular technology does not rely on Wi-Fi access points, enabling service providers to utilize drop-in networking, allowing them to segment services from the healthcare facility's network. Many organizations do not allow third-party access to their central infrastructure due to security concerns. Drop-in networking lets smart healthcare companies provide devices and connectivity without accessing wired or wireless LANs.

The Hybrid Connectivity Approach for IoT Healthcare

An optimal solution involves blending connectivity options. Many use cases benefit from a hybrid approach, leveraging multiple protocols in a single product. For instance, a healthcare provider could give a patient a blood pressure cuff connecting via Wi-Fi or Bluetooth to a home hub. The data is then aggregated and sent via cellular connection to a cloud management platform, ensuring reliable data transmission. Alternatively, a cellular-connected medical device operates autonomously, communicating directly with the cloud and being monitored remotely, ideal for mobile settings.

Finding the Optimal IoT Connectivity Solution

Connectivity is a crucial component of every connected healthcare device. SKYDATA-IoT offers industry insights and expertise to integrate connectivity into your design. We also provide cost-optimized cellular connectivity plans to reduce the total cost of ownership.