The Essential Guide to Connected Healthcare Considerations:
Wi-Fi, Bluetooth or Cellular IoT?
Introduction

Connected healthcare plays an essential life-saving role amid the COVID-19 pandemic. Healthcare workers using telehealth applications shouldn’t have to worry about device connectivity in mission-critical situations. However, in mobile health scenarios such as field hospitals, keeping device connections stable can be challenging. Many smart healthcare devices like monitors and trackers depend on Wi-Fi or Bluetooth to send and receive data. They need to be within range of a cellular phone, internet router or gateway to connect to the cloud and send their data.

In remote healthcare settings, Wi-Fi and Bluetooth might not be enough to provide always-on connectivity for telehealth devices. As cellular IoT coverage becomes ubiquitous worldwide, OEMs consider it a viable alternative for connecting their medical IoT devices.

<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
</tr>
<tr>
<td>The Drawback of Using Wi-Fi and Bluetooth for Connected Healthcare</td>
</tr>
<tr>
<td>Why Use Cellular IoT Connectivity for Smart Healthcare?</td>
</tr>
<tr>
<td>Connected Healthcare Use Case: Alpha Pharma</td>
</tr>
<tr>
<td>Cellular Connectivity Challenges to Consider</td>
</tr>
<tr>
<td>Diagnosing Your Smart Healthcare Device’s Connectivity Needs</td>
</tr>
<tr>
<td>Drop-In Networking</td>
</tr>
<tr>
<td>The Hybrid Connectivity Approach</td>
</tr>
<tr>
<td>Finding the Right Solution</td>
</tr>
<tr>
<td>Request a Project Review or Developer Kit</td>
</tr>
</tbody>
</table>
The Drawback of Using Wi-Fi and Bluetooth for Connected Healthcare

While Wi-Fi is a low-cost solution suited to many situations, it has several drawbacks, including potential security vulnerabilities and coverage limitations. Wi-Fi depends on an intermediary transmitter — the router — to deliver connectivity to end devices. While Wi-Fi routers provide a strong signal in a limited area around the Wi-Fi network created by them, the Wi-Fi network’s footprint is limited in terms of ubiquitous coverage, and obstructions such as brick or cement walls can be problematic.

Bluetooth can reach a 100-meter outdoor range in optimal conditions (although the more recent Bluetooth 5, or BLE5, can deliver a more extended range with lower power consumption). Like Wi-Fi, though, Bluetooth connectivity depends on a local hub to establish and maintain connectivity — most commonly, pairing an end-device with a smartphone.

Why Use Cellular IoT Connectivity for Smart Healthcare?

Cellular connectivity offers advantages over Wi-Fi and Bluetooth in several key areas, including:

Reliability
The pandemic highlights a growing need for reliable telehealth end devices that can maintain stable connections in different locations. For example, a healthcare worker is making a house call to tend to an elderly patient. Suppose the worker’s devices rely on Wi-Fi, and the patient lacks either a broadband internet connection at home or the security credentials to enable the worker’s device on the wireless LAN. In that case, the device won’t be able to access necessary application resources and perhaps not even operate. Wi-Fi devices depend on a working and locally configured router. Bluetooth devices also depend on pairing with a smartphone or other gateway device. Only a cellular connection allows telehealth end devices to stay online without an intermediary connection point, even as they travel from one place to another.

Scalability
Wi-Fi access points limit the number of devices that can maintain a connection at one time. The facility must install additional Wi-Fi equipment to support more devices on the local network. That approach works in specific scenarios, such as scaling slowly in a dedicated facility like a hospital. However, when a healthcare provider wants to introduce many medical IoT end devices at once, cellular provides an avenue to scale significantly without needing to touch infrastructure. With cellular, there are limits to scaling, too, but these are much higher, and there is substantial "intelligence" in the infrastructure to accommodate peaks in demand.

Better Data Access
OEMs need access to anonymized patient data to make the best use of analytics. Healthcare providers can use that data, and connected healthcare providers can collect and resell it to other firms interested, for example, in machine learning. Such data can create risk scores and identify variables in test results that may lead to better patient outcomes. Efficiently gathering patient data can be tricky within a Wi-Fi infrastructure, as firewalls may prevent access. Cellular connectivity allows providers to access anonymized data sets more efficiently while maintaining security and privacy requirements.
Security
Wi-Fi is inherently prone to hacking attacks and cybersecurity breaches. It includes encryption capabilities, but data is only encrypted if they are enabled with Wi-Fi and Bluetooth on network managers to keep up with downloading security patches and updates. On the other hand, cellular data is encrypted by default, and the provider's cybersecurity team manages security updates. While Wi-Fi 6 provides new security features with the introduction of WPA3, cellular networks still offer more robust end-to-end security built into the technology.

Connected Healthcare Use Case: Alpha Pharma

Alpha Pharma, a life science company based in Italy, makes connected glucometers to help patients with diabetes monitor their blood sugar levels. Their Iris Hybrid glucometer integrates continuous glycemic monitoring with artificial intelligence to support patients and providers in treatment efforts. “Managing diabetes requires constant monitoring and decision-making,” says Alpha Pharma CTO Francesco Cannone. “Our devices create a continual link between patients and providers, and our platform’s algorithms predict problems so patients can take preventative action.” The Iris Hybrid relies on cellular connectivity to deliver data from the device to Alpha Pharma’s cloud-based telemedicine platform, Iris Health Care.

From the beginning, the company chose cellular to connect its telehealth devices. They saw several clear benefits, including coverage, versatility and the ability to collect and aggregate better-quality data for providers. Initially, they started with a single local carrier but moved to Telit for broader coverage and the ability to switch between additional carriers when devices travel from place to place. “We needed to connect the devices of people moving around the world, and we couldn’t ask patients to take the extra step of linking their glucometer to a smartphone or finding a Wi-Fi network,” says Cannone. “Cellular allows clients and patients to use our devices everywhere — without needing to take any additional actions to connect.”

Cannone says the company is considering a hybrid cellular and Bluetooth model for future products, creating a way to incorporate other smart healthcare devices and accessories in their health management platform.
Cellular Connectivity Challenges to Consider

Cellular connectivity introduces new possibilities for connected healthcare applications, but it also carries potential challenges. Here are a few to consider:

**Time to Market**
Regulatory compliance for connected healthcare devices is often rigorous and can differ significantly depending on the region of deployment. Around the world, most countries have testing and certification requirements for healthcare devices. In addition to the usual wireless certifications, these medical-grade certifications can significantly increase the time it takes to get a telehealth device from design to market. For example, in the U.S., the FDA device certification process can be long and complicated, with cellular adding a layer of complexity for smart healthcare devices. OEMs also need to seek FCC, GCF, PTCRB and specific operator certifications to operate a cellular device, while Wi-Fi and Bluetooth devices need FCC and Bluetooth SIG certification.

**Design Complications**
Carrier certification and regulatory requirements impact device design, as do the radio frequency (RF) capabilities required. Bluetooth and Wi-Fi are relatively simple, having one or two RF bands to contend with and various antenna solutions. Cellular device design, on the other hand, is far more complicated when it comes to RF. Since devices must be able to connect in different countries with various operators, they might need to support a dozen or more frequency bands giving rise to interference and coexistence engineering design challenges.

**Power Management**
While cellular offers more flexibility and mobility, it consumes more power, particularly if transferring data at Gigabit LTE speeds. Even at lower data speeds, cellular devices need to transmit strongly enough to reach a cell site that may be hundreds of yards away. That effort can quickly drain battery power. New cellular IoT technologies, like Cat-M and NB-IoT, attempt to solve that problem, offering all the benefits of cellular and extremely low power consumption. Intended for intermittent machine-to-machine (M2M) communication, Cat-M and NB-IoT technologies have slower data transfer speeds than other LTE devices. Still, they bring the ubiquitous connectivity feature that neither Wi-Fi nor Bluetooth can offer. Both LTE-M and NB-IoT offer power-saving strategies, such as Power Saving Mode (PSM) and extended Discontinuous Reception (eDRX), that designers can use to extend operating time for battery-powered devices.
Diagnosing Your Smart Healthcare Device’s Connectivity Needs

There’s no one-size-fits-all connectivity option for connected healthcare devices. Instead, OEMs must consider the needs of their use case and find the solution that works best.

When choosing the right connectivity solution for your medical IoT devices, here are a few key questions to consider:

• In what region(s) will the device be deployed? What are the regulations it will need to comply with regarding data privacy and security?

• Is the device usage mostly fixed or mobile? (Will this device be taken with the patient in their vehicle or while they are traveling?)

• How much data will this device consume? (Is it using a large amount of data because of high-definition video or images? Is it sending small amounts of data from a medical device? Does it rely on real-time voice communications?)

• Will there be many devices nearby that need to be connected at once (e.g., a hospital setting)?

• Is the device intended for home health use (if it’s Wi-Fi-based and subject to the patient’s home internet connection)?

• How will the type of connectivity affect device aesthetics, such as antennas?

• Will device location services be needed?
Drop-In Networking

Because it does not depend on Wi-Fi access points, cellular enables a service provider to utilize drop-in networking, allowing IoT providers to segment their services from the rest of the healthcare facility’s network. Many organizations do not allow third-party service providers to access their central infrastructure due to security concerns. When that’s the case, drop-in networking allows smart healthcare companies to easily provide devices and connectivity to a healthcare facility without needing access through their wired or wireless LANs.

The Hybrid Connectivity Approach

For your device, the best solution might be a blend of connectivity options. Many use cases benefit from a hybrid approach, combining the strengths of multiple protocols in a single product. For instance, a patient is given a blood pressure cuff to use at home. The cuff connects via Wi-Fi or Bluetooth to send data to a home hub, where it’s aggregated and sent via cellular connection to a cloud management platform so healthcare providers can access it. This arrangement avoids the complication of seeking a wearable cellular device certification as the wearable itself is not cellular. The hub’s cellular connection ensures a more reliable avenue for data to make its way back to healthcare providers.

On the other hand, a cellular-connected medical device such as a blood pressure monitor that does not rely on connecting to a hub or a smartphone hotspot has the advantages of being fully autonomous. It can talk to the cloud and be monitored remotely and used in a mobile setting such as inside a moving vehicle.

Finding the Right Solution

Connectivity is a pivotal component of every connected healthcare device. Telit offers intelligent insights into the industry and can provide expertise to help you make connectivity an intrinsic part of your design. Telit offers cellular, Wi-Fi, Bluetooth and GNSS hardware modules and data cards and cost-optimized cellular connectivity plans that can lower the device’s total cost of ownership.

Start Your Pioneering Journey with Telit LTE-M and NB-IoT Modules

Request a Project Review or Developer Kit