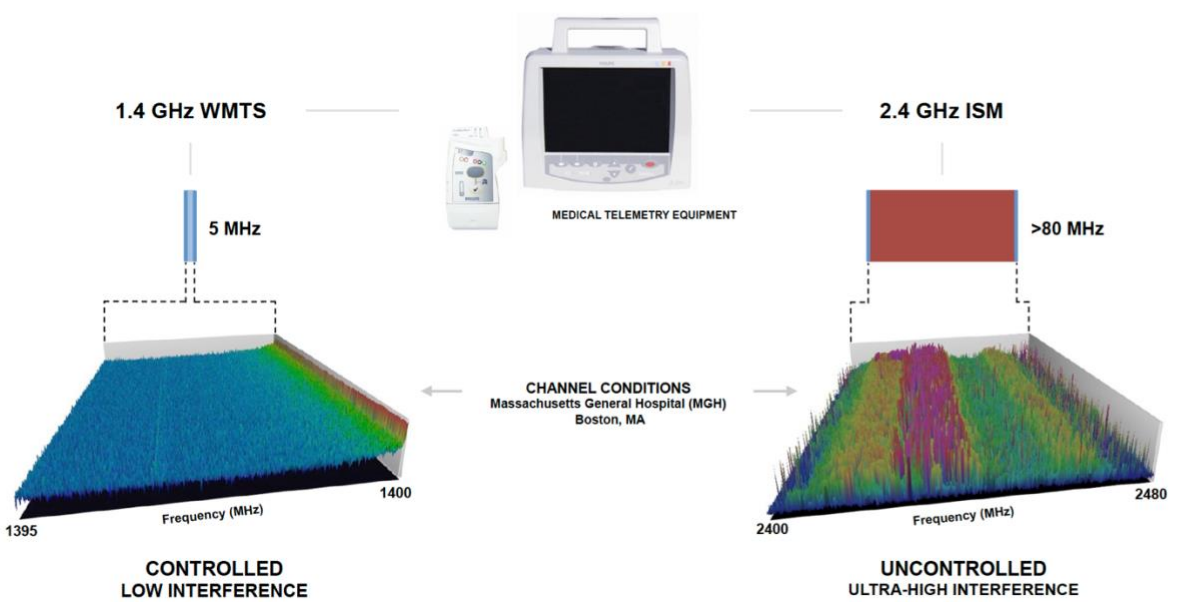
Enhancing patient safety and security

Making the case for licensed spectrum and 3GPP Standardization in wireless patient monitoring

June 17, 2025 by John Dooley, spectrum engineer

Wireless patient monitoring is an important component of modern health care, allowing continuous surveillance of vital physiological parameters such as heart rate, respiratory rate and blood pressure. These systems enable real-time data transmission, which supports timely clinical interventions, reduces patient risk and enhances operational efficiency. However, the reliability and security of the communication infrastructure are critical to the effectiveness of wireless patient monitoring.

Many health care institutions have historically used unlicensed spectrum, such as the 2.4 gigahertz (GHz) and 5 GHz industrial, scientific and medical (ISM) bands. These frequencies are commonly utilized by Wi-Fi, Bluetooth and a large diversity of other protocols, making them prone to interference, security vulnerabilities and interoperability limitations. As the demand for data-driven clinical decision-making increases, continued use of unlicensed spectrum poses a risk to patient safety and operational efficiency.



1

Figure 1: Unlicensed 2.4 GHz ISM spectrum vs. Licensed 1.4 GHz WMTS spectrum –
Even hospitals in dense urban environments benefit from licensed WMTS spectrum, providing a predictable and interference-free medium for transmitting patient biometrics.

Transitioning to licensed spectrum, such as the wireless medical telemetry service (WMTS) at 600 (megahertz) MHz and 1.4 GHz, is necessary to ensure highly reliable and interference-free medical telemetry. However, it is only a first step. Merely shifting patient monitoring functions to WMTS spectrum is not sufficient. Long-term standardization within the globally recognized [3rd Generation Partnership Project] (3GPP) framework is essential to enhance security, ensure interoperability and enable scalable integration with advanced technologies such as artificial intelligence (AI), machine learning and the Internet of Things (IoT). Additionally, licensed spectrum resources like the 3.5 GHz citizens broadband radio service (CBRS) priority access licenses (PALs) should now be considered as a complement to WMTS, permitting carrier aggregation and improved performance of next-generation, high-bandwidth medical applications.

The challenges of unlicensed spectrum in health care

The widespread use of unlicensed spectrum results in significant congestion due to competing devices and networks. In hospital settings, where uninterrupted telemetry is essential for critical patient care, interference can compromise system reliability and patient outcomes. Wireless patient monitoring systems operating in unlicensed spectrum are susceptible to packet loss, latency spikes and transmission delays, increasing the potential for medical errors and delayed interventions.

In critical areas such as intensive care units and emergency rooms, reliable, interference-free connectivity is needed to ensure seamless transmission of crucial health metrics. Unlicensed spectrum, open to various users, cannot guarantee the level of assurance needed for mission-critical health care applications.

In addition to interference-based limitations, security vulnerabilities in wireless medical telemetry arise from the inherent openness of unlicensed spectrum. Many legacy patient monitoring systems use proprietary protocols with minimal security features, making them targets for cyberattacks. The most significant cybersecurity risks include:

- **Unauthorized data access.** Unsecured wireless networks allow attackers to intercept and manipulate patient telemetry data, violating compliance requirements such as the Health Insurance Portability and Accountability Act and the General Data Protection Regulation.

- **Ransomware attacks.** Malicious actors may find ways to compromise medical telemetry networks, disable these networks and demand ransom payments for reactivation.

- **Denial-of-service (DoS) attacks:** Attackers can flood unlicensed spectrum bands with interference, disrupting telemetry transmission and delaying critical care.

Given the increasing frequency of cyberattacks in the health care sector, transitioning to 3GPP-standardized licensed spectrum is imperative. 3GPP-compliant networks incorporate advanced encryption, mutual authentication, and access control mechanisms to protect patient data and ensure the integrity of wireless medical telemetry.

The absence of standardized communication protocols in proprietary wireless telemetry systems leads to fragmented interoperability among different medical device manufacturers. This lack of standardization complicates infrastructure expansion, locks health care providers into vendorspecific solutions and inhibits the adoption of next-generation technologies. Integrating WMTS spectrum within the 3GPP framework would mitigate these challenges by creating a unified standard for wireless medical telemetry. This approach ensures seamless interoperability across different vendors, enhances deployment flexibility and future-proofs health care wireless networks.

Standardizing for enhanced security

The Federal Communications Commission allocated WMTS spectrum at 600 MHz and 1.4 GHz to provide dedicated, interference-free bandwidth for medical telemetry applications. However, despite its regulatory protection, WMTS has not met its full potential due to the absence of a scalable and standardized wireless framework. Incorporating WMTS into the 3GPP ecosystem will enhance its usability, enabling carrier aggregation with other 3GPP bands, such as the Citizens Broadband Radio Service (CBRS), to improve network efficiency and performance.

Service	Frequency Band (MHz)	Bandwidth	Usage	Regulatory Protection
WMTS	608–614	6 MHz	Medical telemetry (patient monitoring)	Exclusive for health care
WMTS	1395–1400	5 MHz	Medical telemetry (patient monitoring)	Exclusive for health care
WMTS	1427–1432	5 MHz	Medical telemetry (patient monitoring)	Exclusive for health care
CBRS	3550–3700	150 MHz	Shared commercial & private LTE/5G	Tiered access system: Incumbent, PAL, GAA

Figure 2: Options for Licensed Medical Telemetry Operations: Medical telemetry services currently have access to WMTS spectrum at 600 MHz and 1.4 GHz. CBRS spectrum at 3.5 GHz can augment these resources, especially in future applications where all bands share common 3GPP standardization.

Carrier aggregation between WMTS and CBRS allows hospitals to leverage multiple spectrum bands, ensuring that mission-critical telemetry data is prioritized over less sensitive transmissions. This capability optimizes bandwidth utilization, enhances redundancy, and minimizes latency, resulting in more reliable patient monitoring systems.

Security benefits of 3GPP standardization

3GPP-compliant networks introduce several layers of security that are crucial for protecting wireless medical telemetry. These include:

- **End-to-end encryption.** Ensures that patient data remains confidential during transmission.
- **Mutual authentication.** Prevents unauthorized devices from accessing the network.
- **Network slicing:** Allocates dedicated resources for medical telemetry, isolating it from non-critical hospital traffic and mitigating cybersecurity risks.

By standardizing WMTS within the 3GPP framework, hospitals can implement a more robust, scalable and future-proof wireless telemetry infrastructure. This standardized infrastructure can support emerging technologies with increasing bandwidth requirements and lower levels of latency tolerance. These include:

- **AI and predictive analytics**. AI-driven predictive analytics rely on high-fidelity telemetry data to identify early warning signs of patient deterioration. Machine learning models use continuous monitoring data to detect abnormalities and recommend proactive interventions. The reliability of these AI-driven applications depends on uninterrupted, low-latency data transmission — something that licensed, 3GPP-standardized spectrum can guarantee.

- **IoT and remote patient monitoring.** IoT-enabled wearable medical devices generate large amounts of real-time data that require secure, high-speed wireless communication. Standardized 3GPP networks facilitate seamless integration of IoT medical devices, allowing health care providers to monitor patients remotely while maintaining stringent security and privacy controls.

- **5G and network slicing.** 5G technology offers low latency and enhanced network slicing capabilities, ensuring that mission-critical telemetry traffic is always prioritized. Hospitals can implement dedicated network slices for patient monitoring applications, preventing interference from nonessential hospital traffic and further improving data transmission reliability.

Protecting patient monitoring devices

Continued reliance on unlicensed spectrum for wireless patient monitoring exposes health care institutions to several risks, including interference, security breaches and network congestion. Hospitals must prioritize transitioning to licensed spectrum, beginning with WMTS at 600 MHz and 1.4 GHz.

However, licensed WMTS spectrum alone is not sufficient. To fully realize the potential of secure and reliable wireless medical telemetry, WMTS must be integrated into the 3GPP ecosystem, enabling carrier aggregation with non-WMTS 3GPP bands like CBRS. This integration will improve network resilience, enhance security and future-proof wireless health care infrastructure.

Collaboration among health care providers, regulatory agencies and other leaders is needed to achieve this vision. By aligning medical telemetry with 3GPP standards, the health care field can establish a secure, scalable and next generation-ready foundation for wireless patient monitoring, ushering in a new era of digital health care transformation.

***John Dooley** is a spectrum engineer, who helped create the E-WMTS patient monitoring solution with TerreStar spectrum. He is a full-time member of the 3GPP standards body and holds numerous patents for wireless device and infrastructure technologies.*