Intelligence and the Internet of Medical Things (IoMT)

Delivering Connectivity and Security in a Wearable Physical Therapy Device

The physical therapy sector has been redefining itself for decades. Its growth trajectory has been fueled by a desire on the part of healthcare organizations to expedite hospital discharge protocols while reducing costs and providing a better quality of service.

As healthcare providers grow into larger entities, their connections to in-network physical therapy practices become increasingly important. But what about the connection to the patients themselves? It wasn't that long ago that every medical device was a standalone tool.
The Science of Recovery

The further emergence of recovery sciences was boosted by necessity in the early 1900s with the unprecedented number of wounded soldiers returning home from the Great War (World War I) and the onset of the polio epidemic. Medical facilities relied upon “reconstruction aides” to serve the recovery needs of those coming out of surgery for wartime injuries. These technicians often came from the fields of nursing and physical education. Over time, formal certifications were offered by institutions such as Reed College in Portland, Oregon and the Walter Reed Hospital in Bethesda, Maryland. The Physical Therapy (PT) Review first appeared in 1921, followed by the emergence of the American Women’s Physical Therapeutic Association (AWPTA) and an increase in research spending for medical recovery devices and exercise equipment.

Following World War II and another massive wave of injuries, surgeries and recoveries, the occupational status of physical therapists shifted from technician to practitioner. The growth in hospital construction around the USA starting in the 1950s contributed to the concept of the “outpatient” and led to a rise in the development of therapeutic tools and devices for hospital and home use.

It’s sometimes said that the work of physical therapists (PTs) stops short-term disabilities from becoming long-term conditions. In addition, PTs are charged with delivering many positive musculoskeletal and circulatory outcomes for those in their care. A PT’s work promotes healing after medical procedures and injuries, and often keeps patients from undergoing more invasive surgeries that can be costly and fraught with risk. Physical therapists have been at the forefront of restoring physical function and movement for their patients, which can directly alleviate some instances of a patient’s overreliance (abuse) of opioids for pain management.

The Intersection of IoT and Patient Data

The proliferation of physical therapy clinics and highly-trained practitioners has been matched by the whirlwind of mergers and acquisitions within the healthcare space, and the evolution of advanced tools and technology. These developments and progress not only require the need for more data storage but the requirement of efficient communication and complete system security.

As hospital organizations and healthcare providers grow into larger entities, their connections to in-network physical therapy practices become increasingly important.

But what about the connection to the patients themselves? We have seen a rise in the usage of smart watches and consumer health apps within the mobile market. However, the promise of secure, connected medical devices outside of a hospital setting is still relatively new. The acceptance of telehealth (the delivery and facilitation of health and health-related services including medical care, provider and patient education, health information services, and self-care via telecommunications and digital communication technologies), in-home physical therapy and the emergence of IoT is hastening a major shift.
What’s Next for Connected Devices?

The ability of caregivers to diagnose and quickly react to medical data by recognizing patterns is mission critical. It saves lives, improves patient recovery outcomes and enhances the quality of life for many millions of people each year.

Given the current head-spinning array of innovations at the intersection of IoT and modern medicine, you might conclude that we are entering the age of the medical internet of things (IoMT). Accelerated by the fact that patient data can now be securely shared among local and remote medical professionals in real time—the next wave of development is happening at lightspeed.

Microchip has been active in the world of wireless connectivity and IoT for many years. We are often called upon to share our expertise as customers envision new capabilities for tomorrow’s diagnostic devices and physical therapy solutions.

“The Internet of Things comprised of smart, connected and secured end nodes is picking up steam.”

Ganesh Moorthy
President and Chief Operating Officer,
Microchip Technology
The Challenge

A leading developer of wearable medical devices approached Microchip with a concept for a home therapy solution that incorporates IoMT connectivity features, intelligence and security.

The company’s physical therapy customers are practitioners in acute care hospitals, long-term care facilities, dedicated medical offices, outpatient clinics, inpatient rehabilitation centers, long-term care facilities, athletic departments and even in the workplace. Physical therapists are offering expert instruction on the movements and exercises required for patients to practice at home and explain the proper use of the medical devices prescribed for home use. The majority of remote or wearable medical devices lack secure connectivity features. This makes it difficult to assess if these devices are working properly when the patient is away from the hospital or clinic. Patient-use compliance has become a big issue for many therapeutic technology products. Healthcare providers simply can’t have too much data about their patients to overcome liability concerns and to deliver positive patient outcomes.
Microchip’s pioneering customer recognized this market opportunity and began to prototype next-generation solutions that would be both technically advanced and provide key enablers for value-based care among physical therapists. Among the key requirements for their new-generation IoMT device:

**Device Functionality**
- Support and execute the proper functions for the appropriate therapy
- Include reliable wireless connectivity so the patient can move freely throughout the day
- Require device battery to be re-charged no more than once per day
- Ability to remotely service and fix issues including updating the device’s firmware

**Device Intelligence**
- Know if the patient put the device on correctly
- Sense and record if the patient puts the device on, takes the device off and at what time
- Monitor if the patient is using the device correctly throughout the day
- Detect any problems with the device that may compromise patient safety, and implement a safe state situation

**Device Security**
- Support a secure wireless connection not susceptible of being hacked

**Device Communication**
- Detect any problems with the device and transmit the problem data to the Cloud Server
- Constantly report data to demonstrate that it is working correctly
Adding a new tier of device intelligence in the equation was native to the Microchip team. Our unmatched portfolio of microcontroller solutions is a key building block for any smart device. An appropriate Microcontroller (MCU) was chosen to perform the complex functions of the physical therapy device. The firmware design required a compiler qualified to the IEC 62304 medical software development standard. Functional safety firmware libraries based on international standards such as IEC 61508 also needed to be available for the microcontroller.

With a robust solution set for the wireless connectivity aspect of the design, the Microchip team significantly reduced time to market for the customer. Our low power IEEE 802.11 b/g/n IoT Wi-Fi® module met the target requirement for battery life. There was no need for the customer to subcontract Radio Frequency (RF) engineering experts for the project. In addition, the device needed to properly interface with one of the major cloud service vendors. From our portfolio of support tools, the Microchip team supplied Amazon Web Services (AWS) cloud connectivity which, further reduced R&D costs.

Our customer mandated that the security features of the new device should be done in a hardware-centric mode, hence less firmware. We showed an embedded offering, which would protect the data transmitted via wireless communications, and prevent unauthorized access to the device.

The new design is securely provisioned to authenticate to any of the major cloud platforms.
The Result

A new, smart wearable product was introduced into the physical therapy market with a variety of features that will greatly improve the practice of remote physical therapy while providing practitioners new data insights to optimize the quality of patient care.

The Microchip team collaborated on the new design by delivering three fundamental IoMT enabling technologies:

- A 32-bit Arm® Cortex-M4 microcontroller with floating point unit
- A global agency certified, IEEE 802.11 b/g/n IoT Wi-Fi module
- A secure element CryptoAuthentication™ device

With an industry-leading microcontroller as the engine driving the demanding smart capabilities of the new product, and Microchip’s advanced solutions for secure communication and data protection onboard, the value of our Total System Solution approach was realized.