

The NDAA Should Protect Medtech Safety for Patients



Derek Herrera | Opinion
September 25, 2026

The National Defense Authorization Act needs to protect those who serve, including by ensuring the military can deliver safe, reliable care when lives are on the line.

That is why language in the House version of the FY 2027 NDAA that could sweep medical technology into a broad “right to repair” mandate is so concerning. This is not merely a technical contracting issue. For patients who depend on complex, FDA-regulated medical devices, the question is simple: Who should be responsible for keeping that technology safe, secure, and reliable? For me, that question is not abstract.

In 2012, while leading Marines on patrol in Helmand Province, Afghanistan, I was shot in the spine by an enemy sniper and was instantly paralyzed from the chest down. After being medically evacuated, I spent months in rehabilitation. Later, I found a new profession as a medical device entrepreneur, founding companies to improve life for people living with urologic conditions.

After my injury, medical technology was not an afterthought. It was part of how I recovered, regained independence, and rebuilt my life’s mission. I used a robotic exoskeleton to stand and walk as I received the Bronze Star despite being completely paralyzed, something that would have been impossible without innovation and technological advances for the field.

Medtech remains critical to my day-to-day life. When I think of how much medtech means to my health, I’m constantly reminded about the level of reliability with which the technology must work exactly as intended. There can be no shortcuts when a life or recovery from a grave injury is at stake.

Device repair and maintenance are a necessity. Patients and providers need devices serviced promptly and properly. The issue is whether Congress should require original equipment manufacturers to release sensitive service materials, software tools, passwords, technical data, and proprietary information to entities that may not meet the same standards for training, quality systems, cybersecurity, reporting, and accountability.

Medical devices used in military and civilian care are sophisticated systems that combine hardware, software, sensors, diagnostics, calibration requirements, cybersecurity controls, and FDA-regulated quality processes. Servicing them is not simply a matter of making them functional. It means returning them to FDA-cleared or approved safety and performance specifications using product-specific training, validated tools, qualified parts, calibrated test equipment, approved procedures, documentation, complaint handling, adverse-event awareness, and cybersecurity discipline.

At my company and others with advanced technologies, it often takes months to train engineers and technicians to fully grasp the system and enable them to repair or service products. Is it realistic or fair for anyone to expect a service member or other personnel to pick up a manual and properly service or repair a device they have never worked on before?

The consequences of poor servicing are not theoretical. In a [report](#) to Congress, the FDA identified more than 4,300 reports involving third-party servicing or replacement parts, including reports associated with 40 deaths and 294 serious injuries.

The FDA noted limitations in that data, but it also underscored the importance of quality management, cybersecurity, and distinguishing proper servicing from remanufacturing.

These risks are heightened in military settings, where the Military Health System serves active-duty personnel, military families, retirees, and other beneficiaries and where cybersecurity, readiness, and trust in equipment are essential. Broad mandates could push sensitive service information beyond controlled channels, creating uncertainty about security, traceability, and accountability.

Supporters argue that broader access to tools and manuals could make repairs faster or cheaper. But that framing leaves out the integrated system that makes safe medical device servicing possible.

Manufacturers maintain training programs, qualification requirements, remote diagnostics, parts logistics, approved repair procedures, cybersecurity controls, device-specific knowledge, complaint-handling processes, and escalation pathways to engineers. Anyone servicing a device should be expected to demonstrate the competence, quality control, security, and accountability needed to protect patients.

Several recent broad state right-to-repair laws have exempted or scoped out medical devices, reflecting concerns about patient safety and cybersecurity.

Congress should apply the same common sense to the NDAA. The defense bill should not create uncertainty around who may access sensitive medical device service information, weaken intellectual property protections that support innovation, or require disclosure of cybersecurity-sensitive materials without enforceable safeguards.

As the founder of a small medtech company, I know how hard it is to move an idea from concept to patient care. For small companies, intellectual property is often the foundation that allows them to raise capital, hire employees, and partner with clinicians. Undermining those protections in the name of repair would weaken the innovation ecosystem wounded service members and other patients depend on.

As a Marine, I also know that accountability matters. You train, you verify, you maintain standards, and you know who is responsible when something goes wrong. Military patients benefiting from medtech deserve no less.

Congress should reject any NDAA language that mandates broad access to medical device service materials without equivalent requirements for training, quality systems, cybersecurity, regulatory accountability, and post-repair performance. If lawmakers want to improve repair, they should focus on timely, high-quality service while preserving the safeguards that protect patients.

The people who serve this country deserve medical technology that is safe, reliable, and secure. The NDAA should protect that trust, not compromise it.

Derek Herrera is founder and CEO of Bright Uro, a company that has created and commercialized the most advanced diagnostic sensors and data science for urology and uro-gynecology.



Available Online:

https://www.realcleardefense.com/articles/2026/09/25/the_ndaa_should_protect_medtech_safety_for_patients_1208237.html



AdvaMed.org



AdvaMed



@AdvaMedUpdate

