The Monthly Pulse
December 2025
BLUE GOAT
CYBER
Blue Goat Cyber's Monthly Insights on Medical Device Security & Global Regulatory Expectations

The Monthly Pulse - December 2025

Blue Goat Cyber
5,326 followers
December 23, 2025

As 2025 comes to a close, all of us at Blue Goat Cyber thank you for your trust and partnership.

We know how much work and investment it takes to move a medical device from concept to clearance, and how essential cybersecurity is to protecting that effort. When done right, cybersecurity doesn't slow innovation. It safeguards it, ensuring your technology remains secure, resilient, and aligned with evolving regulatory expectations.

Looking ahead to 2026, our commitment remains clear: to help you bring secure medical devices to market, and keep them safe throughout their entire lifecycle. We'll continue to deepen our expertise, staying ahead of elevated threats and regulatory scrutiny, and stand beside you as a true partner in protecting patients and the healthcare system.

Thank you for including Blue Goat Cyber in your mission. We wish you a relaxing and safe holiday season and a successful, secure year ahead.

Cheers,

The Blue Goat Cyber Team

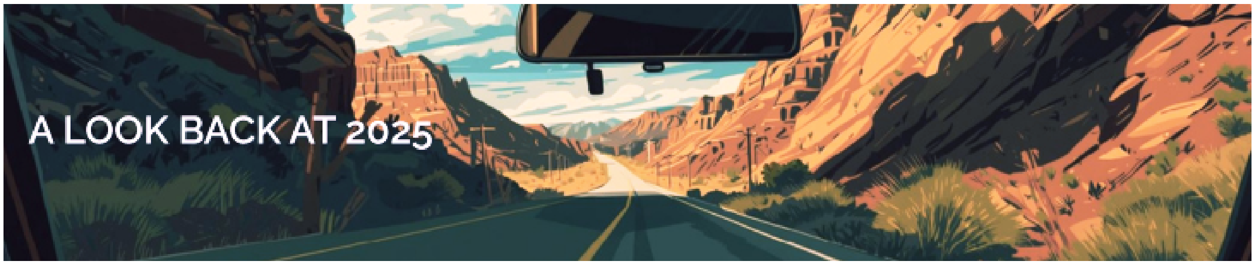
Where You'll Find Us in Early 2026

The Blue Goat Cyber team will kick off the new year in San Francisco at the J.P. Morgan Healthcare Conference, where we are proud to be a Gold Sponsor of the 12th Annual QNova LifeSciences Partnering Forum, taking place January 12-15 at the Hilton San Francisco Union Square. We look forward to connecting with friends, partners, and innovators across the MedTech ecosystem.

We’re also excited to announce that Blue Goat Cyber will sponsor MedTech World Middle East, taking place in Dubai, February 11-13. CEO Christian Espinosa and VP of Strategic Partnerships, Melissa Espinosa, will attend this premier international event alongside global innovators, investors, government leaders, and MedTech visionaries.

As sponsors, we're excited to engage with the community, build new partnerships, and champion the critical role of medical device cybersecurity in the future of healthcare.

If you'll be attending either event, we'd welcome the opportunity to connect.



Regulatory Pulse: What the FDA's Updated Cybersecurity Guidance Really Means

In 2023, the FDA released its first major, comprehensive medical device cybersecurity guidance — a milestone moment for the industry. This June, the agency followed up with an updated version, surprising many by explicitly linking the guidance to Section 524B of the Food, Drug, and Cosmetic Act.

This linkage matters. By tying cybersecurity expectations directly to statute, the FDA strengthened its enforcement authority and clarified several areas that had previously caused confusion. At its core, the guidance emphasizes the need to demonstrate a "reasonable assurance of cybersecurity" as part of medical device safety.

It's important to note: *patient safety* is not synonymous with being "secure" in cybersecurity terms. A device can function as intended while still exposing patients, hospitals, or manufacturers to unacceptable risk.

The guidance reinforces two critical principles:

- A risk-based approach to cybersecurity
- Cybersecurity considerations across the entire device lifecycle, not just at submission

These expectations will require additional development resources, but they also raise the bar for trust, quality, and long-term resilience.

MedTech & AI: What the FDA's AI Data Tells Us, and What It Doesn't

Artificial intelligence is now embedded in the majority of newly released medical devices. In 2025, the FDA updated its AI-enabled device database, listing more than 1,200 authorized devices, up roughly 300 from the prior year.

Notably, none of these authorized devices currently use generative AI (GenAI) or large language models (LLMs), despite the attention those technologies receive in the broader tech landscape.

Most FDA-authorized AI devices today rely on deep learning, with radiology leading the way. Image-based diagnostics continue to dominate real-world clinical use cases.

Could GenAI eventually play a role in medical devices? Possibly. For example, an at-home device might one day generate personalized guidance for patients. But that capability introduces serious cybersecurity risks, including data manipulation or poisoning, that could lead to unsafe or incorrect recommendations.

For now, caution is warranted, and a global regulatory evolution is in play. The challenge is that innovation must be balanced with control, transparency, and patient safety.

Looking Ahead: What to Watch in Medical Device Cybersecurity in 2026

Cybersecurity expectations for medical device approval have become significantly more stringent, particularly with the formal enforcement of Section 524B.

Key questions heading into 2026 include:

- How will enforcement evolve if regulatory agencies face staffing constraints?
- Will submissions be delayed or rejected when cybersecurity assurance appears weak or incomplete?
- How will hospitals, which are already stretched thin, manage increasing dependence on connected technologies?

At the same time, investment is likely to accelerate in areas such as remote care and chronic disease management, where connected devices play a central role. That growth makes cybersecurity not just a regulatory issue, but a foundational requirement for trust.

Blue Goat Cyber will continue monitoring these developments closely, and sharing what they mean for MedTech innovators.

Navigating FDA Cybersecurity Expectations with Confidence

Q: How can Blue Goat Cyber help ensure our new connected medical device meets FDA’s latest cybersecurity requirements, including “cyber device” expectations under Section 524B, so our premarket submission isn’t delayed or rejected?

A: (The Goat): Blue Goat Cyber serves as your dedicated medical device cybersecurity partner, aligning your product and documentation with FDA’s latest cybersecurity guidance and Section 524B requirements.

We support device teams through every step, including threat modeling and security risk analysis, SBOM creation and component analysis, security architecture and documentation, and comprehensive cybersecurity and penetration testing with submission-ready reports.

We also support risk control, residual risk justification, and postmarket needs such as vulnerability monitoring, SBOM monitoring, and coordinated vulnerability disclosure. With a fixed-fee, full-service model and experience supporting hundreds of FDA-regulated devices, we help reduce cybersecurity-related deficiencies and move you through FDA review with greater confidence and predictability.

Have a question for the Goat? Contact us at info@bluegoatcyber.com.

The threats are evolving.

We are vigilant.

We’ve got your back.

Blue Goat Cyber stands ready to help you secure your devices, protect your patients, and stay ahead of the curve — because the stakes are critically high.

Trust. Security. Compliance.

Trusted by Leading MedTech Startups and Manufacturers Since 2014

Schedule a Blue Goat Cyber Discovery Session

Blue Goat Cyber #MedDeviceCyber #MedtechInnovation #Cybersecurity #MedTechDubai2026 MedTech World #FDACybersecurity #AIMedicalDevice QNova LifeSciences #JPM2026