PYA Healthcare Regulatory Roundup #101 – AI-Enabled Medical Devices: New FDA Draft Guidance and Cybersecurity Insights

Presented September 10, 2025 by PYA's Barry Mathis and John Cross | Part of the Healthcare Regulatory Roundup Webinar Series

https://www.pyapc.com/insights/hcrr-101-webinar-ai-enabled-medical-devices-new-fda-draft-guidance-and-cybersecurity-insights/

Please note, this transcript was generated automatically. PYA cannot guarantee its accuracy or completeness.

WEBINAR SUMMARY

In this episode of PYA's Healthcare Regulatory Roundup, experts Barry Mathis and John Cross discussed Artificial Intelligence (AI)-enabled medical devices, U.S. Food and Drug Administration (FDA) draft guidance, and cybersecurity insights. Barry Mathis and John Cross highlighted the evolution of AI, its applications in healthcare, and the FDA's new guidance on AI-enabled medical devices. They emphasized the importance of secure product development, regulatory engagement, and post-market surveillance. A hypothetical smart insulin pump was used to illustrate AI's potential benefits and risks, including model drift and privacy breaches. Key points included the need for detailed documentation, cybersecurity controls, and user education. The FDA's role in ensuring AI devices meet safety and performance standards was also stressed.

Key topics include:

- **AI-enabled medical devices**
- **FDA draft guidance**
- **Internet of Medical Things (IoMT)**
- **Cybersecurity threat evolution in AI-enabled medical devices**
- **AI algorithms**
- **Patient safety and privacy**
- **Smart insulin pump**
- **Medical device model drift**
- **Software Bill of Materials (SBOM)**
- **Predetermined Change Control Plan (PCCP)**
- **Secure product development**
- **Vendor vetting**
- **Threat intelligence**
- **User education**
- **Post-market monitoring**
- **Healthcare compliance**

WEBINAR HIGHLIGHTS AND FREQUENTLY ASKED QUESTIONS

What is artificial intelligence (AI) in the context of medical devices?

- AI in medical devices refers to algorithms and software that can independently analyze data, recognize patterns, and make decisions without continuous human intervention.
- Examples include diagnostic imaging tools, insulin pumps that self-adjust dosing, and devices that detect early signs of disease.
- AI is more than incremental improvement—it represents a fundamental shift similar to the transition from candles to electric light.

How does the FDA's new draft guidance affect AI-enabled medical devices?

- The FDA's 2025 draft guidance builds on earlier cybersecurity rules by making several elements mandatory for AI-enabled and connected "cyber devices." Requirements now include:
- Secure Product Development Framework (SPDF): Risk-based design principles baked in from the start.
- Software Bill of Materials (SBOM): Detailed component inventories, end-of-life timelines, and vulnerability communication plans.
- Lifecycle oversight: Bias mitigation, transparency, labeling standards, and post-market monitoring.
- Change control planning: Predetermined Change Control Plans (PCCPs) to safely update AI models without restarting FDA approval.

Why is cybersecurity now considered patient safety?

- Because medical devices are increasingly connected—via Bluetooth, Wi-Fi, or the cloud—cybersecurity risks directly impact patient outcomes.
- Threats include unauthorized access or ransomware attacks on IoMT devices (e.g., pacemakers, insulin pumps); Model poisoning or data manipulation that could alter device behavior; Denial of Service (DoS) that interrupts critical therapies; and privacy breaches involving sensitive patient health data.
- FDA and industry leaders stress that protecting devices from cyber threats is as essential as preventing falls or ensuring bedside patient ID.

What is "model drift," and why does it matter?

- Model drift occurs when an AI system's predictions shift over time as it learns from new data.
- For example, a smart insulin pump may incorrectly assume a patient always consumes high sugar at certain times, leading to unsafe dosing.
- FDA guidance requires developers to detect and mitigate model drift through performance monitoring and regular updates.

Can you give an example of an AI-enabled device and its risks?

- Yes. A next-generation smart insulin pump combines continuous glucose monitoring with adaptive AI algorithms.
- Benefits include personalized insulin delivery, reduced hypoglycemia and hospitalizations, and better quality of life for patients.
- Risks include hacking via wireless connections, manipulated glucose readings, and algorithm errors leading to dangerous insulin levels.
- FDA requires validation of AI algorithms, documented cybersecurity controls, encryption, threat modeling, and post-market monitoring to manage these risks.

What should healthcare organizations do to prepare for AI-enabled medical devices?

Organizations should:

1. Include IoMT devices in governance and risk programs under the Chief Information Security Officer's (CISO) oversight.
2. Train clinical staff to recognize deviations in AI-assisted care.
3. Conduct regular vulnerability assessments and patch management for medical devices.
4. Vet vendors thoroughly, review contract clauses on data use, and require ongoing compliance audits.
5. Monitor federal threat alerts and integrate third-party intelligence into risk management.

How can developers ensure compliance with FDA expectations?

Developers must:

- Engage with FDA early in the design process.
- Submit detailed pre-market documentation, including SBOMs, performance testing, and cybersecurity assessments.
- Follow an approved PCCP for safe updates.
- Conduct continuous post-market surveillance for model drift and vulnerabilities.
- Provide clear user education on device capabilities, limitations, and security practices.

ACTION ITEMS

- Secure product development: Adopt a systematic life cycle approach for secure product development.
- Regulatory engagement: Engage with the FDA early in the process and follow approved, predetermined change controls.
- Post-market surveillance: Continuously monitor device performance and emerging cybersecurity threats.
- User education: Ensure users are educated on the limitations and capabilities of the AI-enabled devices.
- Include medical devices in risk governance and employee training activities.
- Regularly assess vulnerabilities in medical devices and remediate them.
- Train clinical staff to spot deviations in the care provided by AI-enabled devices.
- Monitor federal alerts for third-party threat intelligence related to medical devices.
- Ensure a deep and trusted partnership with the biomed vendor and support staff.
- Implement proper access controls and patch management for medical devices.
- Thoroughly vet the vendor and review contract clauses related to data usage.
- Regularly audit the vendor to ensure continued compliance and fitness for purpose.

WEBINAR OUTLINE

Introduction and Overview of AI in Medical Devices

- PYA Moderator introduces the webinar, mentioning the topics of AI-enabled medical devices, new FDA draft guidance, and cybersecurity insights.

- Barry Mathis and John Cross are introduced as presenters, with a brief history of their collaboration and experience in the industry.
- Barry Mathis outlines the agenda, including an overview of AI in medical devices, FDA guidance on the Internet of Medical Things (IoMT), and cybersecurity insights.
- Barry shares his experience with cybersecurity, starting from the 1980s, with simple viruses to modern malware and ransomware.

Evolution of Cybersecurity Threats

- Barry Mathis discusses the evolution of cybersecurity threats, from simple viruses in the ‘80s to advanced malware and ransomware today.
- He explains the concept of attack vectors, such as email phishing, and how bad actors exploit vulnerabilities in firewalls and security layers.
- Barry highlights the importance of multiple layers of cybersecurity protection, especially in cloud environments.
- He shares examples of how AI is being used by bad actors to mimic human voices and create convincing phishing scams.

Introduction to AI and Its Applications in Healthcare

- Barry Mathis provides a definition of AI and its historical context, comparing its evolution to the transition from candles to light bulbs.
- He discusses the various types of AI, including generative AI (e.g., ChatGPT) and task-specific AI embedded in medical devices.
- Barry shares a personal anecdote about using AI to generate an Excel pivot table, demonstrating its practical applications in healthcare.
- He emphasizes the importance of AI in improving efficiency and accuracy in healthcare, particularly in radiology and other clinical settings.

FDA Guidance on AI-Enabled Medical Devices

- Barry Mathis introduces the FDA's draft guidance on AI-enabled medical devices and IoMT, highlighting its importance for developers and users.
- He explains the FDA's focus on secure product development, threat modeling, and detailed labeling requirements for AI-enabled devices.
- Barry discusses the regulatory oversight and the need for transparency, bias mitigation, and performance monitoring in AI-enabled devices.
- He emphasizes the importance of post-market monitoring and change management plans to ensure the continued safety and effectiveness of AI-enabled devices.

Cybersecurity Challenges in AI-Enabled Medical Devices

- John Cross discusses the cybersecurity challenges associated with AI-enabled medical devices, particularly those connected to the internet or cloud.
- He explains the risks of unauthorized access, data manipulation, and ransomware attacks on IoMT devices.

- John highlights the importance of cybersecurity controls, such as data encryption, access controls, and regular patch management.
- He shares a hypothetical scenario of a smart insulin pump being hacked, illustrating the potential life-threatening consequences of cybersecurity breaches.

Regulatory Requirements for AI-Enabled Medical Devices

- John Cross outlines the regulatory requirements for AI-enabled medical devices, including the need for a total product life cycle approach.
- He emphasizes the importance of risk-based design, bias mitigation, and transparency in the development and deployment of AI-enabled devices.
- John discusses the need for detailed documentation, performance testing, and cybersecurity assessments in pre-market submissions.
- He highlights the importance of post-market monitoring, change management plans, and user education to ensure the safety and effectiveness of AI-enabled devices.

Impact on Healthcare Providers and Users

- John Cross discusses the impact of AI-enabled medical devices on healthcare providers and users, emphasizing the need for regular risk assessments and vulnerability remediation.
- He highlights the importance of clinical staff training to spot deviations in care and ensure the proper functioning of AI-enabled devices.
- John discusses the need for proactive compliance and regulatory collaboration to ensure patient safety.
- He emphasizes the importance of regular audits, vendor vetting, and contract clauses to ensure the proper use and compliance of AI-enabled medical devices.

Conclusion and Final Thoughts

- Barry Mathis and John Cross conclude the webinar by summarizing the key points and emphasizing the importance of AI and cybersecurity in healthcare.
- The presenters encourage participants to ask questions and seek further information on AI-enabled medical devices and cybersecurity.
- The presenters and PYA Moderator conclude the webinar by thanking the audience and with information on how to access the slides, recording, and additional resources.