A Hands-On Platform for Medical Device Security Education

Kaixin Du
Johns Hopkins University
Baltimore, MD, USA
kdu9@jh.edu

Dibyajyoti Nath
Johns Hopkins University
Baltimore, MD, USA
dnath2@jh.edu

Ramit Saraswat
Johns Hopkins University
Baltimore, MD, USA
rsarasw1@jh.edu

Zhicheng Sun
Johns Hopkins University
Baltimore, MD, USA
zsun54@jh.edu

Michael Rushanan
Harbor Labs
Pikesville, MD, USA
mike@harborlabs.com

Tushar M. Jois
City College of New York
New York, NY, USA
tjois@ccny.cuny.edu

Abstract

Modern medical devices integrate hardware and software, thereby expanding the attack surface and creating patient safety risks. Regulators set cybersecurity expectations, and international standards guide implementation. However, outcome-based, method-agnostic policies give manufacturers wide latitude, producing variability, ambiguity, and fragmented, non-reproducible practices in training and education. We address this gap with a reproducible, open-source reference platform that operationalizes security-by-design in alignment with current regulatory expectations and standards. We also report an initial pilot course using the platform as a foundation for consistent medical-device cybersecurity curricula.

ACM Reference Format:
Kaixin Du, Dibyajyoti Nath, Ramit Saraswat, Zhicheng Sun, Michael Rushanan, and Tushar M. Jois. 2026. A Hands-On Platform for Medical Device Security Education. In *Proceedings of the 57th ACM Technical Symposium on Computer Science Education V.2 (SIGCSE TS 2026), February 18–21, 2026, St. Louis, MO, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3770761.3777308

1 Introduction

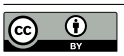
Modern medical devices are complex systems that integrate multiple layers, including analog sensors, embedded processors, firmware, operating systems, drivers, mobile and desktop applications, and cloud services. Recognizing this complexity and the broad attack surface it creates, the U.S. Food and Drug Administration's (FDA) 2025 Premarket Cybersecurity Guidance [3] emphasizes the need for a secure product development framework, or security throughout the medical device lifecycle. Indeed, this guidance was partly motivated by device recalls linked to inadequate cybersecurity design, including the 2019 Medtronic insulin pump recall in which a hacker could remotely change a pump's settings, potentially resulting in an insulin overdose [5].

The same complexity that drives innovation also overwhelms instruction. Students encounter fragmented treatments of embedded systems, networking, cloud computing, machine learning, artificial intelligence, and computer security, often taught in isolation and assessed with paper exercises, case discussions, or narrow lab assignments that do not integrate to demonstrate a complete, secure-by-design process specifically for medical devices. Additionally, classical academic course curricula rarely engage regulatory guidance or industry standards, as they perceived to be less foundational for computer science; nevertheless, these concepts are key to medical device security in the real-world. Further complicating instruction, the guidance defines outcomes without prescribing methods; for example, the FDA/MITRE threat-modeling playbook outlines approaches but does not mandate a specific methodology (e.g., STRIDE, PASTA, attack trees) [2]. The resulting flexibility amplifies uncertainty and contributes to inconsistent practice.

Existing curricula primarily focus on general security, compliance checklists, or academic research. Prior efforts often use medical device cybersecurity as a case study to integrate research and education, and not as the goal of the curriculum itself (e.g. [4]). To the best of our knowledge, no prior work provides a hands-on medical device platform that demonstrates real-world complexity and aligns with regulatory expectations and international standards, including exercises for patient safety and cybersecurity risk management. We attribute the gap to system complexity and to the lack of educational resources that demonstrate a valid, compliant, and reproducible secure-by-design process. Moreover, we believe that the lack of work in this space is emblematic of the difficulties of designing and deploying medical device cybersecurity curricula. Nevertheless, students entering the field are rarely prepared for the cybersecurity work that medical devices require.

Contributions. With the above in mind, we develop a hands-on platform for medical device security education. Unlike static compliance checklists and narrow curricula, our platform provides hands-on, reproducible medical device that aligns with regulatory requirements, offering a foundation for classrooms, labs, professional training, and product development environments. Our contributions are as follows:

- *Open-source reference platform.* A device-to-cloud stack reproducible on commodity components in a lab environment.
- *Secure-by-design workflow.* An end-to-end defined process aligned with prevailing standards (e.g., [1]) and FDA expectations.
- *Regulatory evidence templates.* Worksheets for cybersecurity risk management that meet FDA expectations.
- *Initial pilot.* First class using our platform and worksheets to determine the effectiveness of our approach.



SIGCSE TS 2026, St. Louis, MO, USA

ACM ISBN 979-8-4007-2255-4/2026/02
https://doi.org/10.1145/3770761.3777308

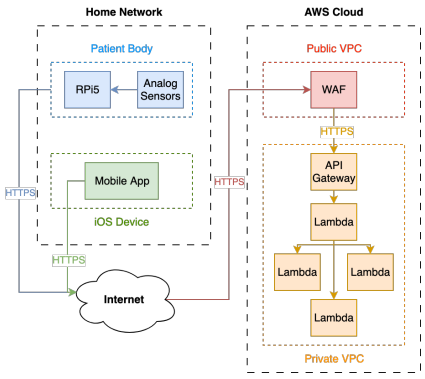


Figure 1: Platform architecture. Note the integration of software, hardware, and cloud components.

2 Design

Our course design aims to teach medical device cybersecurity in a way that is actionable for quality, regulatory, cybersecurity, and product development teams. We target advanced undergraduates and graduate students in computer science, information security, or related disciplines. We emphasize what makes medical devices distinct from general IoT—patient safety. Students should understand that patient safety drives requirements, regulatory expectations, and processes in both the pre- and postmarket phases. Concretely, our platform has the following learning objectives:

- Interpret FDA expectations and relevant international standards to derive safety-tied cybersecurity requirements.
- Apply security-by-design across the device lifecycle.
- Perform threat modeling and cybersecurity risk assessment.
- Implement and verify cybersecurity controls.
- Collaborate on third-party penetration testing to assess residual risk and mitigation efficacy.

Our open-source platform offers a reproducible, device-to-cloud tremor assessment workflow. A Raspberry Pi 5 acquires motion data from accelerometer/gyroscope sensors over GPIO/I^2C and runs a minimal Buildroot-based OS hosting the application. Telemetry is published via MQTT to a cross-platform console that validates and persists records locally. When online, it synchronizes with AWS DynamoDB and S3 for storage, Lambda for event processing, and IAM for access control, supporting remote monitoring, reporting, and configuration. Figure 1 shows the high-level architecture.

We pair the platform with structured worksheets that map FDA premarket expectations to concrete evidence. Students use these materials to produce threat models, trace matrices, and SBOMs. As students iterate on the device, they translate safety-driven requirements into cybersecurity controls, implement and test those controls, and make documented pre-/post-mitigation risk acceptance decisions. The combined platform and worksheets thus operationalize secure-by-design in a hands-on, reproducible way that directly supports the course goals outlined above.

3 Initial Pilot

We offered our first medical device cybersecurity course in Spring 2025 at Johns Hopkins University. The semester-long team project centered on the reference platform, with defined roles (product, security, and regulatory), weekly sprints, and milestone check-ins that required code and worksheets (e.g., PHA, threat model, SBOM) for continuous evidence and timely feedback.

Teams built working prototypes on our platform, extending or refactoring it with different sensors/clients/clouds as needed. Patient safety drove risk assessments and requirements; teams implemented mitigations (e.g., TLS, signed updates) and mapped deliverables to FDA premarket expectations and relevant standards, aligning hands-on work with the course objectives.

The platform proved technically feasible and educationally valuable: students practiced end-to-end secure-by-design and produced artifacts that mirror regulatory submissions. However, we noted that time demands varied – modifying the embedded components was a bottleneck – so future iterations will add tighter rubrics and optional fast paths (prebuilt images, mock sensors) to reduce complexity overheads while still embracing security-by-design.

4 Conclusion

Our platform demonstrates concrete, regulatory-aligned cybersecurity through an open-source, reproducible medical device platform. By coupling a tangible prototype with structured documentation, it transforms FDA expectations into an actionable, secure-by-design process. As both a research reference and an educational testbed, our platform lowers barriers for students, researchers, and practitioners to engage with the realities of medical device cybersecurity across the product lifecycle.

Future Work. We will continue developing our platform via:

- *Educational evaluation.* Deploying in classrooms and training settings under an IRB-approved protocol; quantifying usability and learning outcomes via pre/post assessments, validated surveys, and rubric-based artifact review.
- *Advanced ML integration.* Incorporating real-time health analytics according to the latest FDA ML/AI cybersecurity guidance.
- *Community contributions.* Open-sourcing our materials to solicit feedback from researchers, manufacturers, and regulators.

Acknowledgments

This work is supported by National Science Foundation (NSF) awards 1955172 and 2451597, a Sui Foundation Academic Research Award, PSC-CUNY awards, and awards from Google as a part of the Cyber NYC program. The views contained herein are those of the authors and should not be interpreted as those of the sponsors.

References

[1] 2019. Medical devices — Application of risk management to medical devices. https://www.iso.org/standard/72704.html Third edition.
[2] The MITRE Corporation and Medical Device Innovation Consortium (MDIC). 2021. *Playbook for Threat Modeling Medical Devices.* Technical Report. https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf Prepared for the Food and Drug Administration.
[3] Food and Drug Administration. 2025. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. https://www.fda.gov/media/119933/download
[4] Mehran Mozaffari Kermani, Reza Azarderakhsh, and Mehdi Mirakhorli. 2016. Multidisciplinary approaches and challenges in integrating emerging medical devices security research and education. In *2016 ASEE Annual Conference & Exposition.*
[5] David C. Klonoff. 2019. The First Recall of a Diabetes Device Because of Cybersecurity Concerns. *Journal of Diabetes Science and Technology* 13 (2019), 696–701. https://pmc.ncbi.nlm.nih.gov/articles/PMC6955451/