Statement of Prof. Kevin Fu, Ph.D.

Northeastern University; Boston, MA

College of Engineering
Departments of Electrical and Computer Engineering & Bioengineering; the Khoury College of Computer Sciences; the Kostas Research Institute (KRI) for Homeland Security; and Archimedes Center for Healthcare and Medical Device Cybersecurity

Hospital Cybersecurity and Legacy Medical Devices: Fine Wine or Spoiled Milk?

Submitted to the U.S. House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations Hearing on
“Aging Technology, Emerging Threats:
Examining Cybersecurity Vulnerabilities in Legacy Medical Devices”
Tuesday, April 1, 2025

Executive Summary

Legacy medical devices are inherently insecure, relying on outdated and unsupported software that leave them vulnerable to cyber threats. Essential for patient care, if compromised these devices can disrupt hospitals, adulterate cancer radiation therapy, or cause drug infusion pumps to administer incorrect dosages. Although regulatory efforts have improved medical device cybersecurity, many legacy systems remain unprotected. Flaws in the Contec patient monitor highlight how poor engineering can create significant post-market risks in already cleared devices. The FDA should have greater post-market capabilities to regulate legacy medical devices for cybersecurity risks, as ongoing scrutiny is necessary to protect patient health and prevent nationwide outages of healthcare delivery.

I recommend three actions to improve legacy medical device cybersecurity. First, FDA should grow its cybersecurity expertise to better manage post-market vulnerabilities and emerging threats. Second, Software Bills of Materials (SBOMs) should be strongly encouraged for legacy medical devices to improve cybersecurity incident preparedness. Third, I urge the establishment of national-scale testing facilities, modeled after the NTSB or automotive crash testing, to evaluate medical device security through whole-hospital simulation. These steps enhance national security, promote innovation, and protect patient care.

1. Introduction.

Good morning, Chairmen Guthrie and Palmer, Ranking Members Pallone and Clarke, and distinguished members of the Committee. Thank you for the opportunity to provide testimony on the critical issue of cybersecurity vulnerabilities in legacy medical devices. My remarks today are informed by over 30 years working in healthcare and cybersecurity, and 18 years of fundamental research on medical device cybersecurity. This includes my previous experience as the inaugural Acting Director of Medical Device Security at FDA's Center for Devices and Radiological Health (CDRH).

2. Credentials and Experience.

My name is Dr. Kevin Fu. I represent the academic and healthcare cybersecurity research communities. I am a professor at Northeastern University[1] where I teach medical device security engineering[2] and serve as the Director of the Archimedes Center for Healthcare and Medical Device Cybersecurity. I conduct research on embedded security—the discipline of protecting computers built into every day objects ranging from pacemakers to cars to drug manufacturing. In

[1] Northeastern University is a global campus system in the United States, Canada, and London with a focus on an experiential learning model, high-impact research, deep partnerships, and worldwide reach.

[2] https://spqrlab1.github.io/medcybersecurity/

1993, I worked at a community hospital in Holland, Michigan which introduced me to the challenges and opportunities of maintaining legacy systems in hospitals.

My educational qualifications include a Ph.D., master's degree, and bachelor's degree from the MIT Department of Electrical Engineering and Computer Science. I am speaking today as an individual. All opinions, findings, and conclusions are my own and do not necessarily reflect the views of any of my past or present sponsors or employers.

3. Observations

If we fail to better manage the cybersecurity risks of legacy medical devices, the consequences are not theoretical—they are immediate and potentially life-threatening. In 2008, I co-led a research team that wirelessly exploited a legacy implantable defibrillator, demonstrating how an attacker could induce fatal heart rhythms without physical contact[3]. These are not abstract scenarios. Devices with similar insecurities remain in hospitals today. A bad actor who discovers a vulnerability could disable patient monitors during surgery, spoof vital signs in intensive care units, or hijack infusion pumps to administer incorrect doses.

[3] "A Heart Device Is Found Vulnerable to Hacker Attacks" by Barnaby J. Feder. In The New York Times, Mar 12, 2008. https://www.nytimes.com/2008/03/12/business/12heart-web.html
"Of Fact, Fiction and Cheney's Defibrillator" by Gina Kolata. In The New York Times, Oct 27, 2013. https://www.nytimes.com/2013/10/29/science/of-fact-fiction-and-defibrillators.html

Without proactive cybersecurity measures, including post-market oversight, we risk turning life-saving equipment into attack surfaces that endanger patient safety.

A. Legacy Medical Devices Are Inherently Insecure

A legacy medical device is one that is not merely insecure, but is insecurable. Its software cannot be patched. It is the difference between an unbuckled seatbelt versus a car without any seatbelts at all—unsafe at any speed. While these devices are vital to patient care, many lack the necessary security features to defend against modern threats. They often operate on outdated software and unsupported operating systems, making them vulnerable to attacks that can disrupt clinical operations or endanger patient safety. Unlike consumer smart home devices, failures in medical cybersecurity can have life-or-death consequences.

B. Progress in Medical Device Security

While regulatory and legislative progress has been made to improve medical device security, vulnerabilities still arise, often targeting the weakest link: outdated legacy technology. The pace of advancement has not fully kept up with the evolving sophistication of cyber threats.

C. Cybersecurity Issues in the Contec Patient Monitor

The cybersecurity flaws in the Contec patient monitor are likely a result of poor engineering rather than malice. Applying Hanlon's Razor—never attribute to malice what is adequately explained by stupidity. Short of a wider pattern of subterfuge by a manufacturer, it seems that these flaws are due to negligence. Indeed, history has shown that shoddy engineering in rebranded Chinese products appear driven by business economics rather than subterfuge[4]. However, this does not excuse the lack of proper cybersecurity controls, which pose significant risks to patient safety, regardless of the intent. Hardcoded default passwords and network addresses in some medical devices are a prime example of egregious security lapses. These devices are born insecure by default, creating unnecessary risks.

D. The Importance of FDA Scrutiny for Legacy Medical Devices

A key lesson from the Contec advisory is that FDA scrutiny of legacy medical devices should not exclude devices that were previously cleared. Some medical device manufacturers have argued that certain cybersecurity requirements should not retroactively apply to older devices. However, the Contec advisory illustrates why exempting legacy devices from cybersecurity requirements is

[4] https://www.bunniestudios.com/blog/on-microsd-problems/

detrimental to patient safety. Grandfathered medical devices should not be exempt from security considerations if the goal is to ensure timely, safe, and effective healthcare whether in cardiac monitoring, cancer radiation therapy, or other critical treatments and diagnoses.

E. Need for Independent Testing Facilities for Whole-Hospital Simulation

In my testimony to this Committee nine years ago[5], I emphasized that the nation lacks independent, large-scale testing facilities, such as those comparable to the NTSB (for post-market testing), automotive crash safety testing (for pre-market evaluation), or NNSS (for destruction and survivability testing). Such proving grounds are essential for evaluating the cybersecurity defenses of medical devices in whole-hospital environments.

F. Lack of Visibility and Security Posture Awareness

In a 2018 letter to this Committee[6], I highlighted how hospitals struggle to identify which devices are in use, let alone assess their security postures. Without visibility into the software and components that make up a device—a challenge that Software Bills of Materials (SBOM) seek to address—healthcare providers are left operating in the dark when new vulnerabilities emerge.

[5] https://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-FuK-20161116.pdf

[6] https://spqrlab1.github.io/papers/Fu-Archimedes-House-EC-supported-lifetimes-2018.pdf

G. Cybersecurity as a Solution, Not a Problem

Cybersecurity is not the problem; it is the solution. Robust security measures will enable new markets, promote innovation, and foster consumer confidence in the use of technologies that improve quality of life. Conversely, poor security can erode trust, leading patients and clinicians to lose confidence in technological solutions.

4. Recommendations

I offer three key recommendations to manage cybersecurity risks from legacy medical devices:

A. Preserve and Expand FDA's In-House Cybersecurity Expertise

Post-market vulnerability management requires FDA staff with deep technical expertise in cybersecurity, not just regulatory affairs. These cybersecurity staff crucial to national security are not necessarily pre-market reviewers, but are often **non-review staff** who monitor for and manage newly discovered post-market vulnerabilities and incidents. These subject matter experts (SMEs) are essential for evaluating risks, working with manufacturers on coordinated vulnerability disclosures, and issuing effective guidance. The loss of SME capacity at FDA would seriously hinder national readiness to respond to emergent threats—posing risks to national security.

i. Support agencies such as HHS/FDA, DHS/CISA, DOC/NIST, and NSF to advance our understanding of how to protect legacy medical devices and to establish a cybersecurity workforce that meets medical device industry needs.

ii. Help the FDA retain and recruit cybersecurity talent, not just for pre-market reviewers, but also for post-market management of legacy medical security vulnerabilities and incidents that otherwise will lead to patient injury and harm.

B. Require or Strongly Incentivize Software Bills of Materials (SBOMs)

SBOMs should be required for all new devices and strongly encouraged for legacy devices. These inventories allow stakeholders—including manufacturers, regulators, and hospitals—to rapidly assess whether they are affected by newly discovered software vulnerabilities or exploits.

C. Support Shared Testing Infrastructure for Embedded Cybersecurity

Study the feasibility of standing up an independent, national embedded cybersecurity testing facility modeled after the NTSB, automotive crash safety testing, or the Nevada National Security Site. The U.S. needs a national-scale, independent facility akin to the NTSB or crash test labs—where healthcare providers, manufacturers, and researchers can collaboratively evaluate the security of complex, interoperable medical systems. The cost of not doing so is borne daily by the 6,000+ hospitals each repeating duplicative risk assessments on individual medical devices without shared resources and without the rigor of a whole-hospital simulation.

5. Summary

Legacy medical devices run on outdated software, making them vulnerable to attacks that can threaten patient safety. It is important to preserve and increase FDA's in-house cybersecurity subject matter expertise, not just for medical device reviewing, but also post-market management of vulnerabilities and incidents. Finally, I recommend establishing a National Technical Means in the form of testing facilities to evaluate medical device security through whole-hospital simulation.

Cybersecurity is not a barrier to innovation. It is a foundation. It enables trust in medical technologies, ensures continuity of patient care, and protects public confidence in our healthcare infrastructure. We cannot treat cybersecurity as an afterthought. It must be embedded throughout the entire lifecycle of a medical device from design to decommissioning. Legacy medical device security is spoiled milk, not fine wine. It does not age gracefully.

I thank the Committee for your leadership and attention to this important matter and am happy to support your efforts going forward.

Respectfully submitted,

Kevin Fu

Kevin Fu, Ph.D.

Director, Archimedes Center for Healthcare and Medical Device Cybersecurity

Professor,

Departments of Electrical & Computer Engineering and Bioengineering

College of Engineering

Khoury College of Computer Sciences

Kostas Research Institute (KRI) for Homeland Security

archimedes@northeastern.edu

secure-medicine.org

spqrlab1.github.io

Biography

Dr. Kevin Fu, Ph.D., is Professor of Electrical & Computer Engineering, the Khoury College of Computer Sciences, and Bioengineering at Northeastern University in Boston where he directs the Archimedes Center for Healthcare and Medical Device Cybersecurity. He is also a faculty member at the Kostas Research Institute (KRI) for Homeland Security. His laboratory protects medical devices from cybersecurity threats that could otherwise disrupt patient care. Fu’s 2008 research on vulnerabilities in implantable cardiac defibrillators prompted improvements at medical device manufacturers, global regulators, and international safety standards bodies. His pacemaker research also inspired an episode of Homeland. Before joining Northeastern University, Fu served as the inaugural Acting Director of Medical Device Security at FDA’s Center for Devices and Radiological Health (CDRH) and program director for cybersecurity at FDA's Digital Health Center of Excellence. Fu received his B.S., M.Eng., and Ph.D. from MIT.

Fu’s work has earned him honors, including ACM Fellow, IEEE Fellow, AAAS Fellow, Sloan Research Fellow, MIT Technology Review TR35 Innovator of the Year, a Fed100 Award, and an NSF CAREER Award. He also received an IEEE Security & Privacy Test of Time Award for his pacemaker security research, as well as best paper awards from USENIX Security, IEEE Security & Privacy, and ACM SIGCOMM. Fu has testified in the House and Senate on matters of information security and was commissioned by the National Academy of Medicine to publish a report on trustworthy medical device software. He served as the co-chair of the AAMI cybersecurity working group to create the first FDA-recognized consensus standards to improve the security of medical device manufacturing. Fu advises medical device and pharmaceutical manufacturers on cybersecurity regulations for operational technology.