Executive Spotlight

A Deep Dive Into Upcoming Cybersecurity Legislation With Healthcare Executives

PREPARED BY

EXECUTIVES FOR HEALTH INNOVATION

In 2022, Executives for Health Innovation convened a small group of cybersecurity experts, regulators and policy experts to discuss cybersecurity concerns facing healthcare executives. New guidance and regulations related to medical devices, healthcare systems, and patient data were discussed in detail. The current legislative challenges facing Congress cast a shadow on the entire discussion as the group dived into recent FDA draft guidance and pending legislation. The group identified the top concerns driving executives. A summary of the key concerns and highlights from the discussion are provided below.

KEY CONCERNS OF CYBERSECURITY EXPERTS IN HEALTHCARE

- ***The FDA's Draft Pre-Market Guidance related to medical device security is top of mind for all stakeholders***. Recently, the Food and Drug Administration (FDA) released another round of draft guidance for medical device security. This round incorporated recommendations sent from healthcare leaders and medical device manufactures (MDM). The FDA removed the idea of Risk Tiers, replaced the "Cybersecurity Bill of Materials" with the "Software Bill of Materials," added Investigational Device Exemptions (IDE), and aligned the document with the Secure Product Development Framework.[1]

- ***Addressing medical device cybersecurity is a shared responsibility.*** The expertise of leaders across the industry in both the public and private sector is needed. While some seek to cast blame on one stakeholder, because of the connected nature of the data and systems, a solution cannot be created in a vacuum. Varied input is required to identify the right solution.

- ***Cybersecurity IS compatible with interoperability.*** Some in the industry have suggested that securing medical devices and hospital systems creates a barrier to interoperability. Our experts strongly suggested this is a myth. Secure patient data safe should never impede information sharing. In fact, proper cybersecurity ensures the protection of patient data as it moves between parties.

- ***Congress is working to create sector-agnostic cybersecurity legislation.*** Cybersecurity is a concern for all industries, not just healthcare. The concerns facing healthcare systems are also being faced by the financial, manufacturing, and service industries. Accountability is needed across all businesses. Congressional leaders, like Senator Mark Warner (D-VA) are working on legislation to tackle cybersecurity concerns as a whole and not ad hoc legislation that only solves individual "hot button" issues.

- ***Medical device manufacturers (MDMs) are working to bake security into the design of medical devices.*** An important aspect to the latest draft FDA Pre-Market Guidance is the addition of security measures into the medical device's original design. This is no easy task; this assurance takes expensive, state-of-the-art resources and tools.

[1] https://gardner.law/alerts/cybersecurity-in-medical-devices-new-draft-guidance/

- ***Most small hospitals will not meet industry benchmarks without long-term and sustainable funding mechanisms.*** Small and rural hospitals are already struggling to keep the lights on, care for patients, and update technology. Sending federal grants to these hospitals is not an effective quick-fix for their cybersecurity challenges. Long-term funding is required to bolster these hospitals to meet cybersecurity benchmarks.

- ***Federal and private industry need cybersecurity solutions that can reach every facet of the ecosystem.*** The healthcare ecosystem is full of hospitals and health systems of all sizes, demographics, funding, and workforce; no single solution will work for every hospital and health system. Too often benchmarks, guidance and regulations consider solutions that work better for bigger, heavily funded hospitals.

Does the federal government share responsibility with the private sector to address cybersecurity threats?

Dr. Suzanne Schwartz, FDA: It is an area of shared responsibility and shared ownership. [The responsibility] is NOT [on] one entity, whether on the government or private sector side. Instead, everyone has a part to play here, and it has been the beauty of being able to work together with so many of you who are attending this roundtable, with whom FDA has enjoyed the ability to communicate, coordinate, and collaborate with, to hear out and to dialogue.

Suzanne Schwartz, MD
Director, Office of Strategic Partnerships & Technology Innovation, US Food and Drug Administration

Colleen Nguyen, Sen. Warner's Office: The Senator envisions a system of increased shared responsibility for cybersecurity practices, protection, and hygiene in the healthcare sector. We must ensure communication among agencies handling cyber security and healthcare. The Federal Government should speak with one voice, and agencies should work together.

Colleen Nguyen
Senior Health Policy Analyst, Office of Senator Mark Warner (D-VA)

How does the FDA think about medical device security?

Dr. Suzanne Schwartz, FDA: Firstly, the scope [of this guidance] looks at Quality System Regulation (QSR). We're looking at the risks of that device at large as it connects within one entire system or system of systems.

The importance of thinking about the pre-market design and development process, as opposed to worrying about that at a later stage, is the alignment with the secure product development framework.

[Another point I want to highlight is that the FDA guidance] went into a fair amount of detail regarding what's anticipated. Like, what the FDA wants to see…documentation within the pre-market submission...[This guidance] is taking a much deeper dive, focusing on the importance of manufacturers determining, and therefore documenting and testing, for risk.

Are we incentivizing device manufacturers to build "secure products"?

Seth Carmody, Medcrypt: Healthcare technology makers must focus on solving a healthcare problem, not security. Currently, with this business model, resources allocated to producing secure-by-design products are viewed as a cost center and need budget justification. While market incentives are unoptimized, we do see progress being made because regulators and customers are introducing some market incentives for makers. Makers then need to, in addition to, being experts in their respective clinical domains, develop expertise in the security domain; this is a herculean task and fails for a host of reasons, including that making a secure-by-design device is more art than science.

Seth Carmody
Vice President, Regulatory Strategy, MedCrypt

Jessica Wilkerson, FDA: One thing I want to ensure is underlined in this conversation is that when we say secure products, we talk about a secure healthcare ecosystem beyond devices. There is a temptation to sometimes over-focus on medical devices. Still, we need to securely design lab equipment and mortuary equipment, building systems in hospitals, non-regulated medical devices, and other products, and other technologies in healthcare ecosystems that may introduce cyber risk. [Often some of] those parts of these conversations aren't included.

Jessica Wilkerson, JD
Cyber Policy Advisor with the All Hazards Readiness, Response, and Cybersecurity (ARC) team in the Center for Devices and Radiological Health (CDRH) within the Food and Drug Administration (FDA)

Dr. Christian Dameff, UCSD: One of the things I encourage is that [the industry uses this] information gathering phase to benchmark and level set.

Christian Dameff, MD
Medical Director of Cybersecurity, UC San Diego Health;
Co-Founder, CyberMed Summit

Is it possible to have secure systems and interoperability at the same time?

Jessica Wilkerson, FDA: A mischaracterization of the guidance is that cybersecurity and interoperability are incompatible. It's the opposite. We have seen a need to clarify the relationship between interoperability and cybersecurity and make sure that patients, caregivers, physicians -- the entire sector -- understand that these are not incompatible goals, and in fact, actually strengthen the other.

How is Congress working to address cybersecurity challenges?

Sean Sweeney, Senator Warner's Office: [Senator Warner] wrote the [Internet of Things (IoT) Cybersecurity Improvement Act] of 2020 which established minimum standards for Federal IoT devices in an attempt to move the conversation and improve the cybersecurity of all IoT devices. He co-wrote the Cyber Incident Reporting Act legislation that passed the Senate at the end of last year. We [at the Senator's office] are hoping it'll be implemented relatively quickly... While Congress has taken a sector-agnostic approach to cybersecurity for many years now, [The Senator] has looked at cybersecurity at large, and he sees the need for more targeted legislation in the healthcare space.

Sean Sweeney
Legislative Assistant, Office of Senator Mark Warner (D-VA)

Colleen Nguyen, Senator Warner's Office: [You have to remind legislators] this is not just about data security, and it's not just about HIPPA or a PHI issue. The Senator sees an opportunity to educate his colleagues in the furtherance of moving forward policies that will help patients and the sector broadly....[The Senator's office] has had so many conversations to [learn more about this issue area] -- to learn from all of [the other attendees here] who have been doing this work for so long. [We need] to figure out some levers that Congress and the Federal government can use.

Are cybersecurity challenges different for smaller healthcare systems?

Dr. Christian Dameff, UCSD: In my experience, there's going to be a vast difference in the cyber "haves and have-nots." Therefore, as [the industry] plans out shared responsibility, there's going to need to be small grants given to rural hospitals to [help them] get caught up on cyber[security]. They don't have the infrastructure, and they don't have the personnel.

Sean Sweeney, Senator Warner's Office: [The Senator] knows this will be a different [experience for every] hospital. And he's fully aware we have critical access hospitals in Virginia that we're concerned about and don't want to overburden, but at the same time [the industry] needs to [help them] up their game.

How can policymakers support cybersecurity efforts in healthcare?

Dr. Christian Dameff, UCSD: I would encourage [lawmakers] to discuss more long-term sustainable funding mechanisms through, for example, CMS reimbursement, when tying cyber safety to a continuous revenue stream in meetings and benchmarks.

Erik Decker, Intermountain Healthcare System:
I'm encouraged that our U.S. lawmakers understand healthcare cybersecurity is about patient safety, in addition to data security. Right now, in healthcare cybersecurity, we are a country of 'have and have nots.' As the National Cyber Director, Chris Inglis, says, we must set the system up in a way that "You have to beat all of us to beat one of us." This means a continual stream of government financial support for small and medium-sized healthcare organizations.

Erik Decker
Chief Information Security Officer, Intermountain Healthcare

Technology gets us part of the way, but the largest shortage is in our people and processes to sustain a cyber program; this is why financial support is necessary. It means information sharing. It means shoring up the cyber workforce shortage and establishing loan forgiveness programs for those that work in the health and public health sector. It means looking at cybersecurity comprehensively like Senator Warner is doing.

Greg Garcia, HSCC: Market forces alone will not be able to address the complexity of evolving cyber threats. So, we need CIPAC (Critical Infrastructure Partnership Advisory Council), which has a structure for that. [That structure] is now enshrined in law through the Defense Authorization Act, which prescribes responsibilities among all sector risk management agencies-- not just healthcare-- about how they need to engage with the private sector.

Greg Garcia
Executive Director, Cybersecurity, Healthcare and Public Health Sector Coordinating Council

What areas should be addressed first to ensure patient safety?

Dr. Jeff Tully, UCSD: One of the things that we have to do is think about a healthcare delivery organization as a piece of a more extensive network. [We need to think about] how to take all of the resources and tools developed and informed by experts' expertise, background, and experience, like the ones at this roundtable. We need to transmute that [knowledge] into a usable product that can be implemented across various organizations. And then ultimately, [we need to decide what] interventions will be the highest yield or impact in delivering patient safety outcomes and how we can measure and study those interventions.

Jeff Tully, MD
Assistant Clinical Professor, UC San Diego Health; Co-Founder, CyberMed Summit

What progress has been made in cybersecurity to date?

Dr. Christian Dameff, UCSD: I think so much of the industry success has to do with the people in this room and the work they've done. I know [that the industry] has had many problems, but I want to … say, [the industry] has come a long way in the last ten years. When we started talking about this, it was regarding security researchers getting persecuted by medical device manufacturers for finding bugs.

Now we're discussing the challenging problems and making excellent progress. I want to say I believe that this is because medical devices were the focus at the beginning. It was something tangible. There were a certain number of manufacturers. There was a discrete problem. There was some research in the news. It was something that made tangible sense to a lot of people. You couple that with some outstanding leadership from the FDA, HSCC, and several other federal agencies helping continue to drive a conversation forward and press stakeholders in this space. You have this compelling combination [that can lead to] meaningful change.

What's next? What are you going to do differently in the next couple of months?

Chris Reed, Medtronic: Sometimes it gets overwhelming when we're trying to boil the ocean of legacy medical devices. I'd like to know if we could think and brainstorm a bit more about how we could be more surgical with some of our efforts. It could be very beneficial to drive specific areas of focus for legacy medical devices that may result in the biggest benefit to protecting patients.

Chris Reed
Director of Regulatory Policy, Digital Health and Product Security, Medtronic

Executives for Health Innovation (EHI) is a catalyst for healthcare transformation, convening diverse leaders from across the industry to unlock opportunities for collaborative innovation. As a nonprofit, independent organization, EHI engages in education, thought leadership, and advocacy in cybersecurity and other critical areas. www.ehidc.org

EHI EXECUTIVES FOR HEALTH INNOVATION

EHI thanks Booz Allen Hamilton for their generous support in convening and moderating this roundtable and their continued support of our organization's work addressing cybersecurity challenges in healthcare.

Booz Allen