Post-market medical devices, cybersecurity, and the U.S. FDA's growing concerns

17 January 2018

From insulin pumps and pacemakers to defibrillators, medical devices increasingly rely on wireless and internet connectivity for efficient operations. Unfortunately, these interconnections also leave devices vulnerable to an array of security breaches, hacks, ransomware, viruses, and more. Because many devices are also linked to entire hospital networks, they can be exploited and used as entry points into those larger systems.

In 2016, the U.S. Food and Drug Administration (FDA) issued new recommendations for post-market cybersecurity risk management of medical devices. Hogan Lovells partner Jodi Scott works with medical device developers and users, and knows the potential risks when something goes wrong. In this hoganlovells.com interview, she discusses the FDA's heightened focus on post-market cybersecurity of medical devices, how breaches may threaten patient health and safety, and how companies that build devices can mitigate risk.

The FDA advocates tougher cybersecurity risk management for medical devices. What's driving these recommendations?

Scott: In this day and age, good design principles suggest that you build cybersecurity controls into your software when you build the product. But what's difficult for a lot of companies is that they have technology already out there in the world where, when they designed it five or 10 years ago — some products 25 or 30 years ago — when very few were thinking about cybersecurity. So, from an initial standpoint of how it was created and what they built in it, many companies haven't gone back and retrofitted appropriate cybersecurity measures onto the product. While companies want to ensure that their products are secure and do not present risk to patients and users, there are technological challenges to doing so for older, legacy products.

There are a lot of companies that understand there's a risk with respect to medical devices; they've known for 18 or 20 years that cybersecurity is a risk. To some extent, people naively thought that it would have to be a really horrible, diabolical person to go in and interfere with people's medical devices or their healthcare. As a result, devices were designed and the risks managed for the ordinary user and the most likely scenarios that you would expect to see. But we've gotten past that naïve perspective and now know that there really are people out there who try to breech devices for illicit purposes or simply to see if they can. The device industry is

getting better about managing the risk, identifying the potential for failure, and is now trying to figure out how you manage that risk in something that has been in the market for 20 years while at the same time managing the same risks for product they launch every day. That's where it gets really hard for medical devices.

What type of post-market assessments do we advise for medical devices?

Scott: We tell our clients — both the ones that are in the design and development stage and those who have products in the marketplace — that you've got to go back and look at your cybersecurity and see how you're managing risk. Or let's go one step back: how are you identifying what the current state of your product is, with respect to cybersecurity vulnerabilities? Have you done that assessment? Do you know what your vulnerabilities look like so you can start to make some decisions about what needs to be addressed and how quickly you ought to get it done.

Some companies say, yes, we've assessed it, we know where the vulnerabilities are, and we're working on closing them down. Then there are others that say, yes, we should do something about that, but we've got all these other things, resources are always tight, we'll think about it next year. But the problem is, in the interim period, bad things can happen.

What cybersecurity risks have the FDA most concerned?

Scott: There are a couple of things. Let's say you have a cybersecurity vulnerability: a virus that gets into your software. If the hospital network doesn't have anti-virus software loaded on — and there are hospitals that don't have this software running on their systems, because they say it slows it down — that virus has the ability to travel through the entire network. So you can have a situation where a virus will come in through your product, travel through the network, and maybe it doesn't do something inherently nefarious itself, it just creates a door. Then that door allows somebody else who wants to come in and exploit it, to do that. And because it's traveled through the network, they can pick and choose which product they're going to exploit; for example, they may be looking for patient data. That's a concern from a data breach standpoint. Or, it is conceivable that someone could use that door to affect a device that is delivering therapy and change settings or turn it off altogether.

FDA tends to be less concerned about patient data because other agencies regulate that. But if hackers are exploiting a device that provides treatment, monitoring, diagnosis, or retains the data you use for diagnosis, that's where FDA is worried. They want companies to have mitigated the possibility that someone could get into the device and change data, or change therapy delivery, for example. Or, if it's all digital and you can't tell that the x-rays of a man with cancer in his leg have been swapped out for a man who doesn't have cancer in the leg — that can impact patient treatment. That's what the FDA is concerned about: the data integrity and who is in control of the

devices. They want to make sure that if you've got vulnerabilities in your device, you are controlling them and you're paying attention.

If a client has a device out there but hasn't kept it up to date with current threats, and something happens, how do we help?

Scott: For my team, if that happens, there's the FDA issue: what happened? What are the patient and user risks? What are you going to do about managing the risks? Do we need to issue a customer communication, release a software patch, execute a recall and if so, what does that look like as there are a thousand different ways to address issues that manifest in the field so that you are fully addressing the risk, but also taking care of the customers' needs.

There are also other issues that our cybersecurity team focuses on, which are, if hackers get in, technically speaking, what are you going to do about it? How much other data, such as patient data, has been breached? Every hospital has your social security number if you've been a patient there. If they've got the ability to manipulate data, why would they not also have the ability to grab social security numbers, patient information, or information about a particular patient's healthcare? Where there are medical devices involved, there should be coordination of the investigation and analysis, as well as the decision-making on how to handle a cybersecurity breach, because even if there isn't a real breach, you've got the potential.

So our cybersecurity team focuses more on what happens to the data after someone has penetrated the system, while your team focuses on how the breach affects patient risk?

Scott: Yes, sort of. In a perfect world, companies would be thinking about cybersecurity and mitigating the potential of it in advance, going through their systems and saying, "let's see where we have vulnerabilities, let's pressure-test it, let's look at the system, let's figure out where the problems are, let's catalog them, and then let's figure out from a risk standpoint which are the ones we've got to plug first." Eventually we've got to plug them all, but you can't do everything at once, so let's do it based on risk. Our cybersecurity team has the technical and strategic capabilities to assist with that activity.

Once you have a possible breach, the way our cybersecurity team would look at risk is a little different from the way I would look at risk. If we had a list of medical device cybersecurity vulnerabilities, the cybersecurity team would look at it from a data breach perspective, as to what type of breach occurred, what type of data is vulnerable? Is HIPAA triggered? Are more basic principles of privacy implicated, and so on. I would look at it from the perspective of, what does it mean for patients and users? Could that breach open up the possibility that there could be patient harm — meaning, could they manipulate the device, manipulate the data, or cause the device to stop in the middle of a procedure? I look at it with a very clear focus on possible patient safety and user risk.

So we look at risk differently and make decisions about what we would tackle first from the identified vulnerabilities. I would go after real patient risk and our cybersecurity team would probably agree with that because it's a regulated medical device. But in the absence of it being a regulated medical device, our cybersecurity team might prioritize those vulnerabilities differently.

If clients with a medical device find that they have been breached, what do you recommend that they do immediately, from a patient harm perspective?

Scott: The first thing would be a health hazard evaluation. That's basically a risk assessment that considers clinical (patient safety) risk. There are different things to evaluate for risk; I look at it from the perspective of, what does this mean? You have a breach — what can they do to the data? And if they do that to the data, how does that play out into patient or user harm?

Sometimes the answer is, there's none. Great — then we're just dealing with the HIPAA, privacy, data breach issues, which while undesirable, do not have the possibility of patient harm and are issues that companies can have plans in place to manage. But if there is, now we've got an FDA problem; on top of our other cybersecurity problems, but the agency is going to be very involved in resolving the ones that present safety risk. Additionally, these companies are in the business of patient care and therefore are acutely focused on making sure that they do not harm the very patients they exist to treat.

Of course, if you have potential for actual patient harm, that brings in all the potential liability issues. Let's say, when we were talking earlier about x-rays, you get the wrong x-ray, you can't tell it's for a different patient, and you treat — that's medical malpractice, but that's also product liability. If you had cancer in your foot and the treatment decision was to amputate based in part on the x-ray, and it turns out it wasn't actually your x-ray and they amputated, there's a pretty good chance someone is going to sue. Now, admittedly, most doctors would not make those kinds of treatment decisions based on one isolated piece of information, but things happen when people assume the data they're making decisions on has a high degree of integrity.

The second thing I'd recommend, totally in tandem, would be a root cause analysis. That's your investigation, where you figure out what in the world happened and how big is it. That will help you figure out what to do.

What are some best practices for a root cause analysis?

Scott: There are a lot of methods to use when doing a root cause analysis; it depends on what the issue is. The principle is that you keep asking "why" until you can't ask another "why." They call it "five whys." Why did this happen? Because it wasn't designed to do X. Why wasn't it designed in? We didn't know it was an issue that we needed a plan for in 2018. Well, why? And so on.

The challenge is to make sure you've asked enough "whys" to really drill down into, why did this really happen? Why did nobody recognize it as an issue back then, so we didn't look for it?

So you advise doing a health hazard evaluation and a root cause analysis. Is there anything else you'd recommend that the client do immediately?

Scott: Consider whether you have to notify people. With cybersecurity, you're not usually able to launch a fix right away because it requires some software development work. But there are times when you want to communicate early so that your customer has an opportunity to factor that into their decisions about how they use the product and how they manage their patients. FDA's mantra is: notify early, notify often. Companies probably wouldn't go quite that far, but the idea is, give clinicians the information so they can make a decision based on that particular patient.

Sometimes there are serial communications: you let them know, tell them what the immediate fix is, then tell them later what another fix is. But these people are smart; if you tell them there's an issue, they can factor it into their decision-making. Companies don't love serial communications, because they'd like to do it once and move on. But depending on how big and complex the issue is, as well as the type and seriousness of risk that is presented, sometimes that's how it plays out.

FDA has been talking in a very clear and focused way about cybersecurity for the last few years, but if you think about the thousands and thousands of devices that have already been sold or are in customers' hands, there are pretty significant vulnerabilities that are not a weekend project to remediate. We're talking many, many, many man-hours to get your arms around where the vulnerability is, establish a plan to address it, and then ultimately do it. There's just so much technology out there that is critical to the delivery of healthcare and companies need to spend time working to make sure that it does not become an unnecessary risk. So, they should get started now.

About Jodi Scott

Jodi Scott developed and honed her practical, real-world sensibility and business acumen during the time she spent as an in-house FDA counsel with the world's largest medical device manufacturer. Today, she uses that background to solve the challenges that confront her clients in areas that include quality system compliance, MDRs, regulatory due diligence, importing and exporting medical devices, advertising and promotion, preparing for and managing FDA inspections, and developing systems to mitigate the risks associated with the unapproved use of approved products (aka off-label uses).

Contacts

Jodi Scott

Partner

> Read the full article online