In Conversation With... Jeffrey Shuren, MD, JD

May 28, 2020
In Conversation With.. Jeffrey Shuren, MD, JD. PSNet [internet]. 2020.
https://psnet.ahrq.gov/perspective/conversation-jeffrey-shuren-md-jd

Editor's note: Jeffrey Shuren, MD, JD is the Director of the Center for Devices and Radiological Health at the Food and Drug Administration. Dr. Shuren is a member of the American Academy of Neurology and in his professional role has presented at numerous healthcare professional society conferences. We spoke with him about the role of the Food and Drug Administration in ensuring the safety of medical devices.

Dr. Kendall Hall: Could you please provide a short overview of your background and your current role at the FDA?

Dr. Jeffrey Shuren: I am a neurologist attorney currently serving as the Director of the Food and Drug Administration's [FDA's] Center for Devices in Radiological Health. I've been in this position for about ten years. Prior to assuming this role I was working on policy in the FDA Commissioner's office.

KH: When we think about the FDA's role in patient safety, it seems like we've come a long way. With so many more, and more complicated, devices and more patients using devices at home, how has your role evolved? How has the role of the FDA evolved in terms of device safety?

JS: We are responsible for overseeing all medical devices in the US marketplace and ensuring that they are safe and effective. Over time, our role has evolved in light of what you've pointed out: increasing complexity and total amount of the products on the market. There are about 190,000 different types of devices on the US marketplace. In the past we have had limited surveillance tools available to us. Our role has changed in that we have become more proactive in identifying, addressing, and preventing safety problems related to medical devices. We have become increasingly more collaborative and communicative.

For example, a few years ago we implemented a policy related to the issuance of notifications when we are dealing with an emerging safety signal. There are circumstances where we may not have full confirmation that there is a new or increased safety risk, or we know that there is a particular risk but we have not yet worked out what the appropriate actions are to take, but we believe it is in the best interest of public health to provide that information to patients and providers. We've also increasingly have been including the voice of patients in the decisions that we've made.

We’ve expanded the scope of what we view as “critical” for assuring the safety of products, and that includes the quality of products and manufacturing. We’ve also been advancing innovation to spur the development of safer medical devices. This includes our Breakthrough Devices Program, which covers devices intended to treat or diagnose life threatening or irreversibly debilitating conditions, as well as a new program that we are establishing called the Safer Technologies Program. Under this program, devices that don’t meet all the criteria to be considered a “breakthrough,” but otherwise may be safer than alternative medical products out on the marketplace, would receive the same additional benefits as under the Breakthrough Devices program.

KH: When thinking about surveillance and indicators that potentially unsafe conditions exist, is there a role for collaboration with another agency, such as the CDC [Centers for Disease Control and Prevention]?

JS: Yes. We work with other agencies, including the CDC around topics such as hospital acquired infections and outbreaks. Different agencies may have different tools available to them. In the case of the FDA and medical devices, the surveillance tools we have had historically had important limitations. Our system is based on passive surveillance: we rely on people to identify that a problem occurred and to then take the time to report it to us, or report it to the manufacturer who then reports it to us. Unfortunately, people can miss things, and they are certainly not going to pick up on all associated events, so it may take longer to identify when there is a safety problem.

KH: Is the FDA considering the use of artificial intelligence [AI] and pattern recognition in device safety surveillance?

JS: The limitations we were experiencing with our surveillance tools, as well as the challenge of getting clinical studies after a product is out in the marketplace, led us to develop a strategy in 2012 to establish a national system that leverages data collected as a part of routine clinical care. That system has been branded the National Evaluation System for health Technology, or NEST, and version 1.0 should be launched in 2020. The capabilities of NEST will eventually allow for active surveillance, as well as the use of software analytical tools and AI in the review of electronic data sets. These functions will allow us to identify potentially serious device risks that we did not know of beforehand. We will also be able to monitor for changes in the frequency with which particular adverse events may occur.

Keep in mind, any medical device and any medical product out on the market place will pose some risks – there is no such thing as a risk-free medical device or drug. The issues we are most concerned with are around the key questions, “do the benefits outweigh the risks?” and “do we provide useful information for providers and patients to make well-informed healthcare decisions?” We then want to make sure we have put in place good surveillance tools to capture any new risks or increased risks. NEST will allow us to build up an active surveillance capability in combination with our existing passive surveillance capabilities. Additionally, it will give us the opportunity to address questions using real world data sources, such as device registries or even electronic health records, where previously we would need traditional clinical trials. This can provide us with critical information more quickly and more efficiently. The NEST system is a little unique for FDA in that we don’t own or operate the system. It is being developed by an independent party and the governing structure has representatives from all the key stakeholders in the device ecosystem. You have patient representatives, provider representatives, payers, industry, and government, who all come together around this. With that representation you really have a system that is of, by, and for the device ecosystem.

KH: When events are reported, do you work with that data to look for root causes of the events?

JS: The device maker is responsible for reviewing the adverse event reports they receive, including assessing whether any complaints are associated with their device, and identifying the root cause of the event. However, we will work with manufacturers to help facilitate those analyses. In some cases, we have even looked at devices in our laboratory to try and identify the root cause of a problem, but we are not resourced to do that routinely.

KH: What do you see as the greatest challenge in ensuring device safety?

JS: I think the rapid evolution of technology is one of the biggest challenges. Technology can both solve and create problems. As we are asked to evaluate new science and new technologies, we are always trying ensure that we are keeping up with the science and applying efficient and effective methods for evaluating those new technologies.

KH: When new technology, such as AI, is developing and changing very quickly, how does the FDA approach its review to ensure you have a good grasp on how the technology may be different and what that means for safety?

JS: We deal with new technologies all the time and all moderate- and high- risk devices are reviewed by the FDA before they come to the market place. One of the challenges you see with medical devices is the fact that they can be modified, and in fact often need to be modified, to get the full value out of the device. Those kinds of continued improvements can be very beneficial to patients and are unlike pharmaceuticals, which remain the same over time. In the case of AI, most people are talking about machine learning algorithms that allow technology to learn and be modified. In some cases it can even modify itself. The FDA put out a white paper back in April of last year to propose an approach that could be applied for machine learning AI that would allow for changes to the technology to be made in near-real time in some cases, while still assuring that that device remains safe and effective.

KH: Is the FDA involved in cybersecurity?

JS: We are very involved in cybersecurity. We've issued policy regarding what manufacturers need to do regarding cybersecurity in the pre-market submissions they send us and what they need to do to remain vigilant once their product is out on the marketplace. Cybersecurity raises one of the interesting challenges around safety, although security is different than safety. Some of the challenges come from software technologies, or what we call software as a medical device or SaMD, where the technology really is the software. In these cases, the ability to make frequent changes to the technology is absolutely critical for assuring patient safety for several reasons. One is cybersecurity: manufacturers need to be constantly vigilant for cybersecurity vulnerabilities and threats, and make modifications as necessary to try to stay ahead of the curve. Second, increasingly technologies, predominantly SaMD, are connected to other technologies within a network. Therefore, changes in the network itself, or in other technologies that link to that network, may require that the device maker implement modifications to assure that they remain viable while not adversely affecting the performance of the medical device. That is one of the unique challenges we are seeing in the world of the internet: frequent modifications are becoming necessary to maintain patient safety.

KH: Is there going be a role at some point for the FDA for ensuring connected, networked technologies remain safe? Or is it going to be up to the device manufacturers to put in place safeguards?

JS: We don't have authority over the healthcare facilities and how they may interconnect technologies. What we try to do is make sure that there is information available regarding those interfaces, so that hospitals can take that into account if they are connecting different technologies. On the cybersecurity front, the Department of Health and Human Services and the Department of Homeland Security engage across the healthcare sector to try and deal with these broader network issues. We participate in those efforts to provide a perspective from the medical device side.

KH: What's next on the horizon for the FDA in terms of patient safety or threats to safety?

JS: With regards to medical devices, I think we talked about some of them. There are the security issues, which are not safety issues, but can affect patient safety. There are the challenges we face with increasingly networked technologies. We've also been focusing on select device materials, particularly where a subset of individuals may be predisposed to a hyper-immunologic response to those materials resulting in adverse events, such as in the case of metal-on-metal hip replacement devices. This can lead to adverse effects and device failure. Finally, there are the changes we're making in national capabilities to identify safety issues.

KH: Is there anything we haven't discussed that you think the patient safety community may want to hear about device safety?

JS: I think that what you'll see from the FDA is our continued efforts to expand our partnerships with other parties, including the clinical and healthcare facility communities. This includes our work establishing medical device registries, our increasing work with industry, and also our expanded partnerships with other countries. We facilitate calls with other countries to share information regarding emerging signals that we are seeing, and to hear from them what they are seeing.