

Reproduced with permission from Medical Devices Law & Industry Report, 10 MELR 01, 01/06/2016. Copyright © 2016 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

## *Regulatory Policy*

### **Panelists Say FDA's Role in Regulating Digital Health Field Unclear, Will Continue to Evolve**

BY DANA A. ELFIN

**T**he regulation of mobile medical applications is likely to remain an open question for the foreseeable future, according to speakers at a Food and Drug Law Institute (FDLI) conference in Washington.

As so-called mhealth apps continue to proliferate and the technologies behind them continue to advance, "it'll be quite a few years before we have a handle on this technology and how it's going to be regulated by the FDA, if at all," Jeffrey K. Shapiro, of Hyman Phelps & McNamara P.C. in Washington, said Dec. 10.

Mhealth includes the use of mobile devices such as smartphones and tablets to deliver health-related solutions outside of traditional doctor's office or hospital settings, and also includes cloud computing, said Zachary Rothstein, associate vice president, technology and regulatory affairs at the Washington-based trade association AdvaMed. Digital stethoscopes and wireless blood pressure cuffs are just some examples of this type of mobile technology.

Given the fast pace at which these mobile applications are evolving, it's not necessarily true that the Food and Drug Administration has any special expertise in this area, Shapiro said.

---

**"FDA doesn't have a depth of experience here that necessarily justifies them heavily regulating this area."**

—JEFFREY K. SHAPIRO, HYMAN PHELPS & MCNAMARA P.C.

---

"FDA doesn't have a depth of experience here that necessarily justifies them heavily regulating this area," he said, noting that the exponential growth in the capabilities of both software and hardware in this field, along with the increasing ability to gather and analyze data, means that even app developers have a hard time keeping a handle on it.

Moreover, Shapiro said that the agency's existing regulations—including how it defines who a manufacturer is—aren't necessarily a great fit for the regulation of the digital health field.

For example, the typical model of a company manufacturing a finished device and shipping it to the customer—where there is a clear line between who the manufacturer is and who the customer is, and the product is finished when it is shipped—may not apply to certain types of software.

Stand-alone software that provides clinical decision support, by contrast, is typically customized in close collaboration between the "manufacturer" and the "customer" and the software "learns" over time while in use, Shapiro told Bloomberg BNA in a Dec. 10 e-mail. "Applying the Quality System Regulation (QSR) to this situation is not easy," he said.

"The current FDA regulatory framework was developed before today's sophisticated cognitive computing and mobile and cloud based computing," he added. "Experience has shown that the FDA's almost 40-year-old regulatory framework is a bad fit for much of today's health IT with its networked ecosystems, rapid iterative improvement, deep collaboration between providers and end-users, and focus on clinical decision support (CDS) rather than direct diagnosis or treatment."

Moreover, he said, the regulation of CDS software also poses serious concerns about entangling the FDA in the practice of medicine, an area completely outside of the agency's purview.

**Agency Struggles to Get Its Footing.** Shapiro pointed to the FDA's finalization of a regulation four years ago with regard to Medical Device Data Systems (MDDS)—medical device data systems that transfer medical data digitally—as an example of the agency's struggles in this area (5 MELR 119, 2/23/11).

Although the original MDDS regulation required that such systems comply with postmarketing quality controls, Shapiro said that, in 2015, the agency subsequently realized it didn't need to regulate the systems at all (9 MELR 117, 2/18/15).

"In the space of four years, they realized it was a waste of time to enforce QSR (Quality System Regulation) requirements for these types of technologies," Shapiro said.

The MDDS regulation pull-back, he said, "shows us just how fast this area is moving and, most importantly, it shows us that the FDA doesn't really know what it's doing in this area."

And he said, that has important implications for policy in this area.

**FDA Regulation Could Kill Innovation.** "FDA involvement in the regulation of these products may kill off the innovation that we're looking for," Shapiro said at the FDLI meeting. And he said, subjecting these products to

agency premarket review is likely to impede their development.

“We need time and experience and usage of these devices” in order to get a picture of how this technology should be regulated, he said.

“There will be a role for the FDA in regulating this,” he said, but “it will be fought out between FDA and industry and FDA and Congress.”

But even though the Food, Drug and Cosmetic Act is a very broad statute and could potentially encompass the entire mhealth arena, the agency has already made clear it doesn't want to regulate all of it.

Indeed, a 2013 agency guidance on mobile applications is evidence that the FDA doesn't even want to regulate all mobile health technologies (7 MELR 607, 10/2/13).

In the guidance, the FDA said it wouldn't seek to regulate consumer-use mobile devices, such as smartphones and tablet computers, only “mobile apps performing medical device functions.”

It also said it would exercise enforcement discretion over mobile apps that may meet the definition of a medical device but pose a low risk to the public.

The list of mobile medical apps the FDA said it would focus its oversight authority on are those it said meet the definition of a medical device and pose risks to patients if they fail to work as expected.

The agency defined those apps it would seek to regulate as ones that transform a mobile platform, such as a smartphone, into a medical device; mobile apps that connect to an existing device for the purpose of controlling its operations; and apps that display, transfer, store or convert patient-specific medical device data from a connected device.

But, Shapiro said, the 2013 guidance is “just the beginning of policy” and “is not the final word.”

**Clinical Support Guidance Still Not Out.** Meanwhile, industry is waiting for the long-promised guidance on medical device decision support software from the agency.

Early in 2015, the FDA said it intended to issue the draft guidance on medical device decision support software in 2015, but it's still not out (9 MELR 35, 1/21/15). Clinical decision support software is designed to help physicians make decisions about patient diagnoses.

“It may come next year,” Shapiro said, “but I'm not holding my breath.”

And Congress has gotten involved in the medtech arena, too, with proposed legislation such as the Medical Electronic Data Technology Enhancement for Consumers' Health (MEDTECH) Act and the Sensible Oversight for Technology which Advances Regulatory Efficiency (SOFTWARE) Act pending in Congress (9 MELR 300, 5/13/15).

The MEDTECH Act would exempt low-risk medical software and mobile health applications from agency

oversight (9 MELR 300, 5/13/15). The SOFTWARE Act, unlike the MEDTECH Act, would create for the FDA three new definitions of software: clinical, health and medical software. Under the legislation only medical software would be regulated by the FDA.

And the FDA may be waiting for Congress to act before it issues the medical device decision support software guidance, Shapiro said.

“Congress is probably going to have say here, too,” Shapiro said.

“It's a dance between Congress and FDA on how this is going to be regulated and also on the actual policy,” he said.

**Payment, Science, Cybersecurity.** AdvaMed's Rothstein said that payment, privacy, cybersecurity and scientific proof issues inherent in the medical technology arena only further complicate potential regulation and policy for these products.

For example, Rothstein said, reimbursement policy drives a lot of medical technology adoption, and agencies other than the FDA are also involved in privacy and cybersecurity issues, he said.

But where cybersecurity threats are concerned, the FDA is “being proactive” in the medical technology arena, Sonali Gunawardhana, an attorney with Wiley Rein LLP, said.

For example, in late July the agency said a pump used to infuse drugs at a patient's bedside can be hacked through hospital wireless networks, causing an over- or under-dose. The pumps were manufactured by Hospira Inc. and called Symbiq (9 MELR 493, 8/5/15). In the fall of 2014, the agency released a final guidance recommending that device companies submit documentation to the FDA about the risks identified and controls in place to mitigate cybersecurity risks (8 MELR 671, 10/15/14). That final document was based on a draft from the summer of 2013 (7 MELR 409, 6/26/13).

Also in the fall of 2014, the FDA held a workshop on cybersecurity, at which federal officials said health-care organizations and device manufacturers should share more information with each other about medical device security (8 MELR 734, 10/29/14).

The agency will be holding another workshop on cybersecurity issues in January (09 MELR 24, 12/9/15).

Among the security vulnerabilities the agency has identified in the area of device cybersecurity are malware threats, uncontrolled distribution of passwords and lagging security patches and updates.

“They're very concerned with this area,” Gunawardhana said.

To contact the reporter on this story: Dana A. Elfin in Washington at [delfin@bna.com](mailto:delfin@bna.com)

To contact the editor responsible for this story: Brian Broderick at [bbroderick@bna.com](mailto:bbroderick@bna.com)