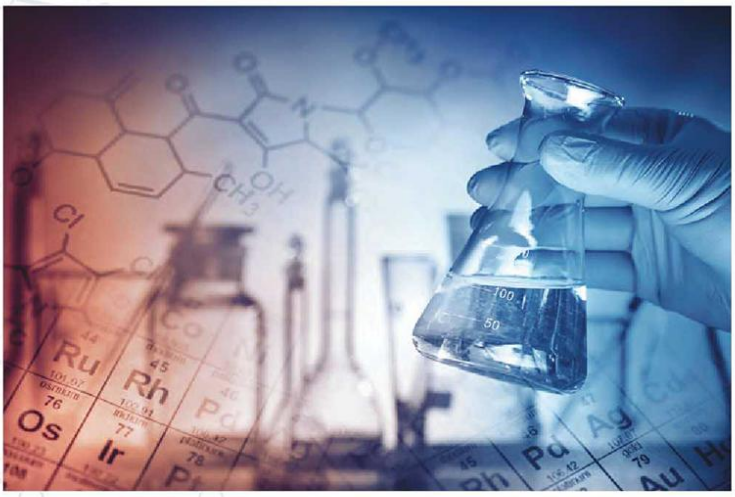
SECOND ANNUAL
PHARMA LAW CONFERENCE



MARCH 3, 2016

CO-SPONSORED BY:

NEW YORK STATE BAR ASSOCIATION
INTERNATIONAL SECTION

KPMG

NYC MedTech
NYC Medical Technology Forum

CORPORATE LAWYERING GROUP LLC

FORDHAM UNIVERSITY
COMPLIANCE AND ETHICS SOCIETY
PROFESSIONALIZING COMPLIANCE

TROUTMAN SANDERS

ATLANTA BEIJING CHARLOTTE CHICAGO HONG KONG NEW YORK ORANGE COUNTY PORTLAND RALEIGH
RICHMOND SAN DIEGO SAN FRANCISCO SHANGHAI TYSONS CORNER VIRGINIA BEACH WASHINGTON, DC

PRIVACY ISSUES WITH THE FDA IN MOBILE HEALTHCARE, CONNECTED DEVICES, AND THE INTERNET OF THINGS[1]

By Mark C. Mao and Ryan Lewis

Introduction

On January 22, 2016, the Food and Drug Administration (FDA) issued draft guidance (the "Guidance") clarifying its recommendations for addressing post-market cybersecurity vulnerabilities in medical devices.[2] While the guidance is a draft only and not enforceable, it does represent the FDA's current thinking regarding manufacturers' responsibilities to monitor, identify, and address cybersecurity threats for "connected" and "smart" medical devices.

By its terms, the Guidance applies to: "1) medical devices that contain software (including firmware) or programmable logic, and 2) software that is a medical device…The Guidance does not apply to experimental or investigational medical devices.[3]

Three particularly notable facets to the issued guidance stand out. First, the FDA emphasizes the importance of information sharing in managing cybersecurity risk to medical devices. Second, the Guidance reinforces the FDA's advocacy of "privacy-by-design" in the manufacture of medical devices for post-market application. Finally, the draft guidance acknowledges the dynamic nature of medical device cyber threats, sets priorities for managing those threats, and in doing so implies certain standards of care.

1. Information Sharing and ISAOs

The FDA suggests in the Guidance that manufacturers may accrue benefits if those involved in the production of the medical device lifecycle share information regarding cyber vulnerabilities and threats.[4] The FDA notes that the exchange of such information is part of the "shared responsibility" of cybersecurity risk management among the medical device manufacturer, the device's user, the Information Technology (IT) system integrator, Health IT developers and other IT vendors providing products not regulated by the FDA.[5]

In order to incentivize such information sharing among entities in the medical device field, the FDA suggests that those entities join Information Sharing Analysis Organizations

---

[1] The contents of this article are merely academic. No one should rely on this article as legal advice, and no attorney-client relationship is created hereto.
[2] Guidance, "Postmarket Management of Cybersecurity in Medical Devices", p. 4, January 22, 2016, U.S. Department of Health and Human Services, Food and Drug Administration, Available at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022
[3] Guidance, p. 7.
[4] *See* Tseng, Elaine H., and Haas, Alexander K., "Medical Device Cybersecurity: What Pharma Cos. Should Know" February 2, 2016, available at www.law360.com/articles/752963
[5] *See* Id. (Tseng).

("ISAOs").[6] Manufacturers that voluntarily join an ISAO may be exempt from certain FDA reporting requirements.[7] In essence, ISAO member manufacturers will be looked upon favorably in the event of a cyber breach.[8]

In conjunction with the Guidance, the FDA has sought public comments on questions relating to ISOAs. The FDA was clearly unsure of how it would confer benefits for participation in ISAOs, as evidence by the nature of the questions asked, and much remains to be determined after public comments are collected.

2. Privacy-By-Design

While the Guidance is primarily concerned with post-market issues, it is clear that so called "privacy-by-design" remains an important element in a manufacturers' threat assessment.[9] As part of its premarket considerations, the FDA urges that manufacturers should "address cybersecurity during the design and development of the medical device."[10] It is evident, however, that preemptive design measures are meant to mitigate post-market developments. "Manufacturers should consider the incorporation of design features that establish or enhance the ability of the device to detect and produce forensically sound post-market evidence capture in the event of an attack."[11]

3. On The Standard of Care

Another interesting aspect of the Guidance is the statement on the standard of care. The states "[b]ecause cybersecurity risks to medical devices are continually evolving, it is not possible to completely mitigate risks through premarket controls alone."[12] The FDA further urges manufacturers to characterize cybersecurity vulnerabilities as "acceptable or unacceptable" and "controlled or uncontrolled".[13] Those characterizations functionally acknowledge that post-market cyber threats are not predictable and totally preventable. In short, the Guidance

[6] *See* Id. (Tseng). As the Guidance explains, ISAOs are the product of "Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing (EO13691), released on February 13, 2015".
103 EO 13691 also mandates that the ISAO
[7] Guidance at
[8] *See* Guidance at 20 ("If the company took this action to mitigate the risk within 30 days of learning of the vulnerability and is a participating member of an ISAO, FDA does not intend to enforce compliance with the reporting requirement under 21 CFR part 806.").
[9] A good example of the importance of "privacy by design" is the recent case of the Federal Trade Commission (FTC) against ASUS. In February of 2016, the FTC settled its claims alleging that ASUS misled consumers about the security of its routers and cloud services, which also constituted unfair business practices. (Press Release, *ASUS Settles FTC Charges That Insecure Home Routers And "Cloud" Services Put Consumer Privacy At Risk* (FTC Feb. 23, 2016).) The FTC noted that it brought the action against ASUS because it was expecting wider adaptation of the internet of things, where home routers and cloud services would play critical roles. The FTC indicated that it believed that ASUS' routers were particularly vulnerable to hacking, that its cloud services did use secure connections or encrypt traffic, and that ASUS' software update tool inaccurately promised the most current updates.
[10] Guidance at 11.
[11] Guidance at 24.
[12] Guidance at 11.
[13] Guidance at 13.

recognizes that privacy incidents are not themselves indicative of a breach of the standard of care.

Instead, as guidance to medical device manufacturers assessing product vulnerabilities, the FDA urges that "such a process focus on assessing the risk to the device's essential clinical performance by considering:

1. The exploitability of the cybersecurity vulnerability, and
2. The severity of the health impact to patients if the vulnerability were to be exploited.[14]

The Guidance then provides particular pointers to assist manufacturers in assessing these two factors, all with the aim of evaluating the overall risk to the device's essential clinical performance.[15]

Additionally, the Guidance provides clarity as to manufacturers' prospective duties to report updates and patches made in response to a perceived vulnerability. Currently, the only remedial actions that will require prompt reporting to the FDA are those intended to correct vulnerabilities affecting the "essential clinical performance" of a device or that "present a reasonable probability of serious adverse health consequences or death."[16] Patches and updates meant to strengthen cybersecurity defenses generally need not be reported.[17]

Conclusion

The Guidance is encouraging for the burgeoning connected medical devices industry, particularly as the "internet of things" continues to develop. The policies and comments laid out by the FDA, certainly indicate that the FDA intends to encourage, rather than stifle, the development of new technologies and services.

The FDA acknowledges the changing and unpredictable nature of cyber threats, and instead focuses on whether the manufacturers are managing "acceptable" risks. Thus, the FDA focus on the design, as well as the collective reassessment of the manufacturers.

[14] Guidance at 13.
[15] Guidance at 13-15.
[16] *See* Overley, Jeff, "FDA Details Cybersecurity Steps for Approved Med. Devices" January 15, 2016, www.law360.com/articles/747440
[17] Guidance at 17.