April 21, 2016

Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Room 1061
Rockville, Maryland 20852

RE: Comments of ACT | The App Association regarding the Food and Drug Administration's Draft Guidance, *Postmarket Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff* (Docket No. FDA-2015-D-5105)

ACT | The App Association writes to provide input to the Food and Drug Administration (FDA) on its draft guidance on managing postmarket cybersecurity vulnerabilities for marketed medical devices.[1] For the United States to realize the potential mobile health apps hold, the companies that stand positioned to avail their innovations to the healthcare space require transparency in legal and regulatory responsibilities. ACT | The App Association applauds the FDA for its leadership in promoting scalable and flexible cybersecurity management policies and appreciates this opportunity to provide input.

ACT | The App Association represents more than 5,000 app companies and technology firms that create the apps used on mobile devices around the globe. As the world has quickly embraced mobile technology, our member companies have been creating innovative solutions across modalities and segments of the economy, with healthcare as a prime example. Through our Connected Health Initiative (CHI), we clarify outdated health regulations, incentivize the use of remote patient monitoring, and foster an environment where patients and consumers can see improvement in their health.[2] This coalition of leading mobile health companies and key stakeholders works with Congress, the FDA, the Center for Medicare & Medicaid Services (CMS), and other key policymakers to promote policies that encourage mobile health innovation while keeping sensitive health data private and secure.

[1] *Postmarket Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff; Availability*, 81 FR 3803 (Jan. 22, 2016) ("Draft Guidance").

[2] http://connectedhi.com/.

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org

I. General Views of ACT | The App Association on the FDA's Draft Guidance

Connected medical devices have the potential to radically improve the American healthcare system. With over 60% of the population already using mobile apps to help track their conditions and make informed choices about their health,[3] mobile-app enabled telehealth and remote monitoring of patient-generated health data (PGHD) continues to represent the most promising avenue for improved care quality, reduced hospitalizations, avoidance of complications and improved satisfaction, particularly for the chronically ill.[4]

While the rise of the Internet of Things through an ever-increasing amount of Internet protocol-enabled products (including medical devices) holds great promise, this environment also faces increasing security threats due to a broadened attack vector, necessitating more evolved and dynamic risk management practices. No data is more personal to Americans than their own health data. ACT | The App Association members appreciate this and put extensive resources into ensuring the security and privacy of sensitive health data to earn and maintain the trust of consumers, hospital systems, and providers. Fully leveraging technical measures including end-to-end encryption, as well as utilizing trusted channels for information sharing, are a critical element to accomplishing this.

We appreciate the FDA's leadership and work to provide clarity and guidance regarding cybersecurity vulnerabilities in the postmarket context and its efforts to build on the White House's Executive Order and related Presidential Policy Directive addressing America's critical infrastructure and its resiliency to attacks.[5] These foundations, and the voluntary, flexible, and scalable National Institute of Standards & Technology's Cybersecurity Framework risk management tool later developed as a result,[6] promote a harmonized approach to cybersecurity risk management for critical infrastructure, further supplemented by ANSI/AAMI/ISO 14971:2007/(R)2010, Medical devices – Application of risk management to medical devices. Additionally, ACT | The App Association agrees with the FDA that "security-by-design" – the concept of building security concepts into hardware and software from the developmental stages to the "end of life" – is a cornerstone of protecting patient safety in this new landscape.

---

[3] Get Mobile, Get Healthy: The Appification of Health & Fitness Report, Mobiquity (2014), *available at* http://www.mobiquityinc.com/mobiquity-white-papers?ref=mHealth-report-2014.

[4] *See, e.g.,* Hindricks, et al., The Lancet, Volume 384, Issue 9943, Pages 583 - 590, 16 August 2014 doi:10.1016/S0140-6736(14)61176-4.

[5] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739 (Feb. 12, 2013); Presidential Policy Directive/PPD-21, Directive on Critical Infrastructure Security and Resilience, 2013 Daily Comp. Pres. Doc. No. 00092 (Feb. 12, 2013).

[6] National Institute of Standards & Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

II. Specific Views of ACT | The App Association on the FDA's Draft Guidance

Based on the above, ACT | The App Association provides the following specific recommendations in response to the FDA's Draft Guidance.

a. ACT | The App Association Supports the Draft Guidance's Approach to Cybersecurity Routine Updates

ACT | The App Association notes its support for the FDA's proposed approach to routine cybersecurity software modifications. Given the dynamic world of threats and responses that occur and are addressed in software, software modifications are needed constantly. Software developers understand and take seriously the potential damage to patients and make great efforts to keep such products as effective and secure as possible. These updates almost universally have no bearing on the medical application of the device and are strictly security-themed. To overzealously require reporting requirements for these changes would negatively affect the medical device manufacturers and healthcare providers that rely on them.

As far back as 2005, guidance from the FDA, which the Draft Guidance is intended to supplement, has addressed software maintenance actions required to address cybersecurity vulnerabilities for networked medical devices. Specifically, for medical devices that incorporate off-the-shelf ("OTS") software, the FDA has stated that medical device companies will very likely not have to report updating software in medical devices with cybersecurity patches because "most software patches are installed to reduce the risk of developing a problem associated with a cybersecurity vulnerability and not to address a risk to health posed by the device."[7] Consistent with this approach, in the Draft Guidance the FDA proposes to clearly state that medical device software changes made to strengthen cybersecurity will generally not be required to be reported. We support the FDA's retention of this approach moving forward.

[7] FDA, *Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software* (Jan. 14, 2005) at 5.

b. The FDA Should Reconsider its Proposed Establishment of "Essential Clinical Performance"

In the Draft Guidance, the FDA proposes to establish the concept of "essential clinical performance" in the postmarket context.[8] From the perspective of ACT | The App Association, the software development community which has relied on the FDA's guidance documents is unfamiliar with this term. Its introduction into FDA regulatory considerations would introduce unnecessary complexity into the software lifecycle process, as decisions around the level of performance necessary to achieve freedom from unacceptable clinical risk is defined in the concept/design/premarket phase of the software lifecycle. Based on these concerns, ACT | The App Association recommends that the FDA remove its proposed introduction of "essential clinical performance" from the Draft Guidance.

c. The FDA Should Fully Embrace Trusted Information Sharing Fora to Improve Postmarket Cybersecurity Management

ACT | The App Association also agrees with the FDA on the key role of information sharing in postmarket cybersecurity management. The voluntary timely sharing of cybersecurity threat indicators among stakeholders from both the public and private sector will be crucial in the detecting, mitigating, and recovery of cybersecurity threats. While we congratulate the FDA on its partnership with the National Health Information Sharing & Analysis Center (NH-ISAC), we urge the FDA to make clear that participation in the NH-ISAC should not be promoted to the exclusion of Information Sharing Analysis Organizations (ISAOs), which are envisioned to be formed to fill needs for unique communities, large and small, sometimes across economic segments. The rise of ISAOs as a complement to Information Sharing Analysis Centers (ISACs), of which the NH-ISAC is one, helps to address the resource limitations of small- and medium-sized entities as well as the convergence of business models that may make it difficult to determine which ISAC to engage.

Therefore, ACT | The App Association urges the FDA to provide further clarity in its guidance on postmarket surveillance that engagement with an ISAO that meets the criteria set through the Department of Homeland Security,[9] including but not limited to the NH-ISAC, be considered in alignment with the approach and incentives related to information sharing in the Draft Guidance. The necessity for this approach is reflected throughout the FDA's discussion in the Draft Guidance, such as the instance where FDA notes that "[cybersecurity signals] may also originate in another critical infrastructure sector (e.g., defense, financial) but have the potential to impact medical device cybersecurity."[10]

---

[8] Draft Guidance at 12-13.

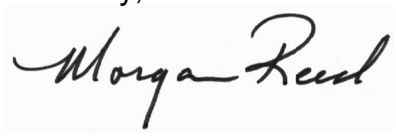
[9] https://www.dhs.gov/isao.

[10] Draft Guidance at 9.

III. Conclusion

ACT | The App Association appreciates the opportunity to provide input to the FDA on its Draft Guidance. The FDA is encouraged to contact ACT | The App Association with any questions.

Sincerely,



Morgan Reed
Executive Director
ACT | The App Association