July 24, 2018

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


To Whom It May Concern:

The Advanced Medical Technology Association (“AdvaMed”) appreciates the opportunity to provide comment on the Food and Drug Administration’s (“FDA” or “Agency”) Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health (“Plan”).\(^1\) AdvaMed represents manufacturers of digital health technologies, medical devices, and diagnostic products that are transforming health care through earlier disease detection, less invasive procedures, and more effective treatment. Our members range from the smallest to the largest medical technology innovators and companies.

We applaud the FDA’s recent initiatives to promote patient access to innovative new therapies and diagnostics while maintaining the Agency’s safety priorities. The Center for Devices and Radiological Health’s (“CDRH”) shift to a total product life cycle (“TPLC”) organizational structure exemplifies these forward-thinking initiatives. Integration of staff members whose experience combines review of innovative devices with methods to monitor and promote device safety serves CDRH’s vision of patient access to high-quality, safe, and effective medical devices of public health importance first in the world. As CDRH moves to a TPLC organizational structure, continuing to work with industry members to assure device safety will remain important. Below we offer our comments on the various initiatives discussed in the Plan.

1. Establish a Robust Medical Device Patient Safety Net in the US

Real world evidence (“RWE”) may provide FDA, industry, providers, and patients with robust evidence on product safety and effectiveness that accurately reflects how products are used and experienced in the real world. AdvaMed continues to support FDA’s efforts to use RWE in its regulatory decision making and its collaboration with the National Evaluation System for Health Technology Coordinating Center (“NESTcc”). The NESTcc represents an important multi-stakeholder public-private partnership that can be a catalyst to drive the development of RWE through infrastructure development, data governance policies, and the

use of reliable methods to ensure the validity of evidence. The NESTcc is creating
distributed networks of collaborations and partnerships that will link together diverse real-
world data (“RWD”) sources (e.g., health systems, payers, and registries) to access data
already generated by our health system to support the evaluation of medical products’ safety
and effectiveness. The NESTcc will also be responsible for ensuring that appropriate
policies and safeguards are in place to maintain patient privacy for RWD accessed through
the network. The reliability of the RWE generated through the NESTcc will be dependent
upon robust analytical methods. To address this challenge, the NESTcc is also establishing
communities of highly qualified experts to identify the appropriate analytic methods to be
used to ensure that the RWE generated through the NESTcc is reliable, high-quality and
meaningful to FDA and other stakeholders.

By establishing these critical infrastructure and methodological capabilities, the NESTcc will
evolve to support innovative active surveillance approaches that should identify potential
safety signals faster and reduce potential harm to patients. As the ability to conduct reliable
active surveillance grows, continued reliance on passively generated surveillance systems
should decrease. FDA should therefore assess the comparative utility of existing passive
surveillance systems, such as summary malfunction reporting and device tracking
requirements, to identify opportunities to reduce redundancy and improve the quality of
surveillance data broadly. Continued use of redundant surveillance systems is inefficient and
benefits neither FDA nor its stakeholders.

2. Explore Regulatory Options to Streamline and Modernize Timely
Implementation of Postmarket Mitigations

We understand that FDA’s proposal to impose special controls through an umbrella
regulation is preliminary and contains limited details. Still, this proposal raises important
concerns. First, it is unclear to us if FDA can implement such an effort under existing
authorities. And assuming that FDA has the requisite authority, the merit of FDA’s proposal
is unclear. Notice-and-comment rulemaking serves a critical and long-recognized purpose:
where agencies propose actions that may have far-reaching and unexpected effects, those
agencies must solicit and consider input from stakeholders who will bear the effect of those
actions and whose insights may otherwise be unavailable. This is a virtuous process that
does not prevent agency action; it simply predicates action on development and consideration
of available relevant data.

We of course understand that rulemaking may be time-consuming and complicated by
bureaucratic process. But we would suggest that the solution is not to unilaterally end
rulemaking. Rather, FDA should identify and overcome whatever internal obstacles prevent
efficient practice. Our concerns in previous policies proposed by FDA, such as the release of
draft guidance on the use of emerging signals in regulatory decision-making, is illustrative.²
In that case, we raised numerous issues with the proposed policy, including FDA’s failure to

---

² See AdvaMed Comments (March 29, 2016) in response to Docket No. FDA-2015-D-4803: Public Notification
of Emerging Postmarket Medical Device Signals (“Emerging Signals”); Draft Guidance for Industry and Food
and Drug Administration Staff; Availability, available at https://www.regulations.gov/document?D=FDA-
2015-D-4803-0021.
seek input from the device manufacturer to evaluate an emerging signal. Without the opportunity to comment, the evaluation of emerging signals may have not included criteria that would permit the manufacturer to provide the Agency with important information. (We note that at the time of this submission, our members’ experience indicates that FDA’s current use of emerging signals is subjective and, at times, lacks appropriate input from the manufacturer.)

Should FDA proceed with its umbrella-regulation proposal, it should first explain to stakeholders what this proposal entails and how it differs from current practice. We also ask FDA to provide a formal mechanism for stakeholders to comment on the proposal—and for FDA to consider those comments—before proceeding.

3. Spur Innovation Towards Safer Medical Devices

Safety is the number one priority for the medical device industry. We therefore disagree with the Plan’s statement that “[t]he marketplace . . . does not provide strong incentives to make an established device safer in the absence of a new or greater-than-previously-understood safety concern.” The Plan also suggests that FDA may explore actions that would provide more streamlined pathways for comparative safety claims. Because FDA is not typically involved in reviewing or approving comparative safety claims, it is unclear why a streamlined pathway is needed.

FDA also states that it will seek to establish a voluntary 510(k) pathway for certain moderate-risk devices that would allow manufacturers to use objective performance criteria to demonstrate substantial equivalence. We are concerned with the Agency’s implication that this proposed, voluntary program may signal that certain devices are “safer” simply because they use this program. FDA fails to show how use of objective performance criteria, compared to use of a predicate device, would enable comparative claims of better performance or a safer device. Indeed, ample evidence shows the safety of devices marketed based on substantial equivalence to a predicate.

We would anticipate that objective performance criteria would reflect appropriate clinical need, that there would be a documented, publicly available record of the basis/support for FDA’s determination of what constitutes appropriate clinical need, and that exceeding performance criteria would not necessarily indicate that a device provides a greater clinical benefit. We are also concerned that any claims of superior performance based solely on performance criteria, without comparable increases in clinical performance, could be misleading. Accordingly, we believe that, while a voluntary 510(k) program may enhance efficiencies in some cases, such a program must be transparent and consistent and make no qualitative distinctions between devices cleared via predicates or performance criteria.

4. Advance Medical Device Cybersecurity

A. Build capability to update and patch device security into a product’s design
FDA’s guidance on cybersecurity for premarket submissions states that manufacturers are to submit a summary plan for providing updates and patches when the device is in the market. As a result, device manufacturers already consider these issues during the premarket phase, and FDA reviews the plan prior to clearing or approving the product. It is unclear what more FDA seeks to require considering the existing guidance and expectations that are in place.

Nevertheless, we agree that a manufacturer’s risk management process should include steps to evaluate security risks and, when appropriate, implement security risk control measures that may include design features that support updates and patches. To the extent the existing policy described in the premarket guidance is insufficient, FDA should publish revised guidance to inform industry of the Agency’s policy. Statutory and/or new legal authorities are not needed.

We also believe that, consistent with the notion that cybersecurity is a shared responsibility, the responsibility to perform various types of updates and patches must be clearly understood between the customer and manufacturer at the time of purchase. This will set expectations about who is responsible for defining and completing remediation plans, when necessary. This is consistent with the 2017 Health Care Industry Cybersecurity Task Force Report, which recommends health care delivery organizations and their accreditation organizations to better incentivize such remediation plans.

B. Develop a Software Bill of Materials (“SBOM”) that must be provided to FDA as part of a premarket submission and made available to medical device customers and users.

Requiring SBOMs to be submitted to FDA as part of a premarket submission may be a reasonable step to ensure that manufacturers have implemented basic configuration management processes. In order for SBOMs to serve as a useful tool, all manufacturers should be required to develop them for in-scope products. Requirements to submit an SBOM to FDA should be established by regulation, and we believe that for an SBOM to be useful, its contents and structure must be common across all manufacturers. As a result, the content and structure of an SBOM should be established through a standards setting body to promote a consistent approach both domestically and globally.

Based on conversations our industry has had with health care providers, including those during round-tables hosted by the House Energy & Commerce Committee, the extent to which an SBOM would benefit a customer is unclear. In fact, some health care delivery organizations have indicated that sharing SBOM information would be unmanageable for the thousands of devices operating in their environment. As a result, we do not believe it is appropriate for FDA to require manufacturers to provide SBOMs to their customers. FDA would likely need new authorities to require this type of information to be provided to customers and device users because an SBOM is not product labeling under Section 201(k) of the Federal Food, Drug and Cosmetics Act.

It is also imperative that FDA and the healthcare sector establish procedures to mitigate the potential for the information contained in an SBOM to be used in a malicious manner. In this
regard, there may be a period of time in which a device could be at heightened risk for exploitation after the discovery of a vulnerability—until it is mitigated—if the information contained in an SBOM is obtained by a nefarious actor. To ensure appropriate risk management is in place and unintended consequences are mitigated, limitations should be imposed on the access to SBOM information, such as permitting only hospital network operators access to the information.

In light of these concerns, we recommend FDA convene a multi-stakeholder workshop to examine the benefits and risks of providing SBOM information to customers and device users.

C. Explore the Development of a CyberMed Safety Analysis Board (“CYMSAB”)

The Plan provides limited details of the proposed CYMSAB. It is unclear, for example, what functions FDA would task the new entity to perform. It also appears that discussions within the CYMSAB would likely involve highly sensitive and company confidential information about device technologies. Should FDA establish a CYMSAB, it must not become a separate or parallel regulator to the FDA. FDA must remain the single source for establishing medical device cybersecurity policy and administering and enforcing it.

We are concerned by the Plan’s suggestion that the CYMSAB would “deploy” to investigate suspected security compromises. The CYMSAB’s makeup, selection, authority, training and expertise is not clear, and the notion that it would be granted power to inspect or investigate real world vulnerability events and make decisions requires further discussion.

If FDA believes a CYMSAB could be helpful as an advisory committee to provide recommendations on policy or on technology developments, industry would be supportive, provided that the group includes industry representation, is assembled in an open way, and operates consistent with the Federal Advisory Committee Act, as appropriate.

* * *

AdvaMed would like to thank the FDA for its ongoing work related to medical device safety and looks forward to continuing to work with the Agency on these important issues. Please do not hesitate to contact me at 202-434-7224 or zrothstein@advamed.org if you have any questions.

Respectfully submitted,

/s/

Zachary A. Rothstein, Esq.
Associate Vice President
Technology and Regulatory Affairs