Combination Products Coalition

1227 25th St. NW #700
Washington, DC 20037
combinationproducts.com
202.861.4199

VIA ELECTRONIC SUBMISSION

July 6, 2022

Dockets Management Staff (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Re: Docket No. FDA-2021-D-1158; Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff

Dear Sir or Madam:

The Combination Products Coalition ("CPC")[1] welcomes the opportunity to provide comments on FDA's "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions - Draft Guidance for Industry and Food and Drug Administration Staff" (the "draft guidance").

The CPC greatly appreciates FDA's efforts to provide this draft guidance which helps to establish Agency expectations for the types of cybersecurity activities and evidence required to gain approval and maintain medical devices. Our coalition represents members developing a range of products, including combination products with embedded software and software as a medical device ("SaMD") applications which may be labeled for use with drug or biological products, and therefore has a vested interest in the Agency's expectations regarding cybersecurity.

The CPC's comments on the draft guidance are captured below. The comments are organized by topic along with a discussion and rationale for our proposed change (if applicable).

[1] The CPC is a group of leading drug, biological product, and medical device manufacturers with substantial experience and interest in combination product issues. One of our top priorities is to work collaboratively with FDA on issues affecting combination products and digital products to advance our common mission: providing the best possible health care to patients. Our diverse, cross-industry membership permits the CPC to bring a special, broad, and unique perspective to these issues.

Comments Regarding Applicability of Draft Guidance to Drug Primary Mode of Action Combination Products and Software Used with Drugs

The preface of the draft guidance lists only CDRH and CBER as the Agency centers that have endorsed the content of the document. As the Agency is aware, combination products as defined in 21 CFR part 3 may have software or firmware medical device constituent parts that receive premarket approval under drug marketing applications and combined use of drug products and software is becoming increasingly common. However, CDER is not listed as an endorsing center and Section II. of the draft guidance, "Scope," does not list drug or biological product investigational or marketing application types (e.g., IND, NDA, BLA) as being applicable.

Releasing new digital health guidance without CDER's endorsement presents a challenge to the combination products industry as that center has primary review responsibility for drug primary mode of action ("PMOA") combinations which include digital or software components and it is not clear if the draft guidance will apply to those drug-PMOA combination products.

CPC respectfully requests that the Agency centers collaborate more closely on the final version of the draft guidance to provide meaningful information regarding the applicability of the draft guidance to sponsors of combination products containing software/firmware with a drug primary mode of action as well as to sponsors of medical device software/firmware which are used in combination with drug products.

Comments Regarding Applicability of the Draft Guidance to Investigational Programs

Appendix 3 of the draft guidance, "Submission Documentation for Investigational Device Exemptions," describes the Agency's expectation for cybersecurity evidence to be included as part of the review of Investigational Device Exemption ("IDE") applications. The appendix requests that IDE sponsors prepare and submit a number of cybersecurity elements as part of their application and goes on to suggest that the Agency reserves the right to request and review additional articles of cybersecurity evidence, as appropriate, for the particular device under investigational review.

The CPC believes the policies described within Appendix 3 introduce undue burden on the investigational device sponsor, and by extension, patients, as the sponsor's ability to efficiently and effectively study investigational device technologies is impacted. The CPC would like to raise the following specific concerns.

<u>Lack of Risk Based Approach</u>

The Agency's proposed list of cybersecurity evidence/elements required at time of IDE filing appears to apply equally to any investigational device that incorporates software/firmware systems. The policy does not appear to change based on consideration of the intended use or risk of the product. The CPC recognizes that cybersecurity concerns may be appropriate to examine during the clinical investigation of, for example, an implanted cardiac device; however, the same level of cybersecurity process and documentation should not apply to systems that are low risk, non-implanted, and/or not life-sustaining.

Need for Clarity on Cybersecurity Practice and Process Expectations

The draft guidance discusses expectations for both the cybersecurity processes to be applied by sponsors and the articles of evidence (documentation) which are generated from those processes. Appendix 3 of the draft guidance describes the Agency's expectation for cybersecurity evidence to be included as part of the review of IDE applications, however the appendix does not specify if the broader cybersecurity processes required by the draft guidance are expected to apply to investigational devices, and if those processes would be subject to inspection.

Consideration of Available Study Mitigations

In mandating that certain cybersecurity elements are required for investigational devices, the draft guidance does not appear to recognize that the conduct of clinical studies provide unique considerations in the use of medical devices which makes them less vulnerable to information security threats. For example, the distribution numbers associated with investigational products is often a fraction of commercially approved devices, investigators are required to maintain close oversight of the use of the product, and the patient often receives specialized training and periodic evaluations by the investigator. These factors should be carefully considered by the Agency in authoring the final version of the draft guidance, and, ideally, IDE sponsors should be permitted to provide rationale that cybersecurity evidence of the type the Agency proposes requesting is not appropriate.

*** * ***

Again, the CPC greatly appreciates FDA's efforts to provide this proposed guidance and the opportunity to comment on elements which impact combination product manufacturers. Implementation of the comments and proposals suggested within this letter will greatly assist the combination products industry in understanding the Agency's expectations to applying cybersecurity practices to software and firmware products that are used in combination with drugs and/or are regulated as drug PMOA combination products.

Yours truly,

Bradley Merrill Thompson,
On behalf of the Combination Products Coalition