mdpc medical device privacy consortium

21 April 2015

Docket No. FDA-2015-D-5105 for *Postmarket Management of Cybersecurity in Medical Devices*
Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Room 1061
Rockville, MD 20852

Re: MDPC Comments on Draft Guidance concerning Postmarket Management of Cybersecurity in Medical Devices (Docket No. FDA-2015-D-5105)

To Whom It May Concern,

These comments are submitted on behalf of the Medical Device Privacy Consortium’s (“**MDPC**”) Working Group on Product Security (“**Working Group**”). The MDPC is a group of leading companies addressing health privacy and security issues affecting the medical device industry. Members of the MDPC manufacture a diverse range of products, from molecular diagnostics to medical imaging equipment to implantable devices, for example.

The Working Group commends the FDA for recognizing the need for effectively managing postmarket cybersecurity vulnerabilities for marketed medical devices and appreciates this opportunity to comment on the FDA’s proposed Guidance regarding Postmarket Management of Cybersecurity in Medical Devices (“**Guidance**”).[1]

General Comment

- The Working Group proposes that the FDA remove the concept of “essential clinical performance” from the Guidance. First, this is a new term was not included in the FDA’s guidance on *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* or any other FDA guidance previously issued. Second, defining a medical device’s “essential clinical performance” and resulting severity outcomes if compromised will prove extremely difficult, particularly in complex situations and environments, and could lead to unintended consequences (such as reporting all vulnerabilities regardless of risk). For example, an *in vitro* diagnostic analyzer may be a Class I medical device, but it may run 300 or more

[1] These comments are being offered on behalf of the following Working Group members: Abbott Laboratories, Medtronic, and Royal Philips.

different assays with different intended uses. The impact of a given vulnerability on the device's essential clinical performance may differ depending on the particular analyte tested and/or the intended use of the results.

If the FDA includes the concept of "essential clinical performance" in the final Guidance, the Working Group proposes that the FDA revise its definition to align with the term "essential performance" found in IEC 60601-1 (which requires compliance with ISO 14971) as follows: "*Essential performance* means performance necessary to achieve freedom from unacceptable risk of a clinical function, other than that related to basic safety, where a loss or degradation beyond the limits specified by the manufacturer results in unacceptable risk. Compromise of the essential performance can produce a hazardous situation that results in harm and/or may require intervention to prevent harm."

- The Guidance recommends that device manufacturers apply the NIST Framework for Improving Critical Infrastructure Cybersecurity ("**NIST Framework**") in the development and implementation of their comprehensive cybersecurity programs. The Working Group believes that the NIST Framework is a valuable resource with respect to the management of cybersecurity-related risks and *should* be leveraged by manufacturers when developing and implementing their respective cybersecurity programs. However, the NIST Framework is designed for and applicable to owners and operators of critical infrastructure *generally*, which includes organizations from an array of sectors such as communications, energy, defense, food and agriculture, nuclear, transportation and others. Although the medical device industry shares many of the same cybersecurity concerns as organizations from these various sectors, medical devices also include many unique challenges that are equally important to a comprehensive cybersecurity program and which may be missed if too much emphasis is placed on adherence to the NIST Framework. Accordingly, the Working Group recommends that the Guidance should address the significance of universally-recognized approaches to risk management that are tailored to medical devices (*e.g*., ISO 14971, ISO 80001, AAMI TIR57, etc.). The Working Group further recommends that to the extent there is a conflict between the NIST Framework and recognized approaches to cybersecurity risk management that are tailored to medical devices, deference to such other approaches should be given (or at least taken into account).

<u>Section II (Background)</u>

- In some instances, end users may integrate legacy devices into their networks even though such legacy devices were never designed or intended to be integrated into a network. This, in turn, may create vulnerabilities. The Working Group proposes that the Background to the Guidance should address the postmarket reporting obligations for medical devices that are not designed or intended to be integrated into a network, but if integrated by an end user, may result in new vulnerabilities.

Lines 147-148

- The Working Group proposes that the Guidance should provide more clarity as to the obligations of medical device manufacturers for non-medical information technology that is interconnected with a medical device, including interoperable devices, off-the-shelf technologies and other third-party technology/devices.

Lines 198-202

- The Working Group proposes that the Guidance should include signals originating from third-party suppliers of hardware or software technology, as well as non-security-centric researchers, and thus the Working Group proposes the following change: "A cybersecurity signal could originate from traditional information sources such as internal investigations, postmarket surveillance, or complaints, ~~and/or~~ security-centric sources such as CERTS (Computer/Cyber, Emergency Response/Readiness Teams), ISAOs and security researchers*, suppliers of software and hardware technology, and/or other researchers and professionals*."

Line 264

- End users of medical devices are not always in the clinical setting, and thus the Working Group proposes the following change: "FDA recognizes that medical device cybersecurity is a shared responsibility between stakeholders including health care facilities, patients, providers, *other device end users,* and manufacturers of medical devices."

Line 269

- End users of medical devices are not always in the clinical setting, and thus the Working Group proposes the following change: "Effective cybersecurity risk management is intended to reduce the risk to patients *and other end users* by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity."

Lines 273-278

- As discussed in the Working Group's General Comment above, the Working Group believes that only recommending the application of the NIST Framework fails to address the unique cybersecurity issues applicable to medical devices and the recognized approaches to cybersecurity management that are specific to such devices (*e.g.*, ISO 14971, ISO 80001, AAMI TIR57, etc.). Accordingly, the Working Group recommends that the Guidance should address the significance and role of recognized approaches to risk management that are tailored to medical devices.

Lines 344-347

- Based on the Working Group's General Comment above, the Working Group proposes the following change: "It is recommended as part of a manufacturer's cybersecurity risk management program that the manufacturer ~~incorporates~~ *review* elements ~~consistent with~~ *of* the NIST Framework for Improving Critical Infrastructure Cybersecurity (*i.e*., Identify, Protect, Detect, Respond, and Recover)."

Lines 354-355

- The Working Group seeks clarification as to what the FDA expects from manufacturers with respect to assessing a vulnerability's "future impact" on essential clinical performance. Under what standard, if any, should "future impact" be assessed?

The MDPC welcomes the opportunity to provide the FDA with comments on its Guidance concerning Postmarket Management of Cybersecurity in Medical Devices and appreciates the FDA's consideration. Please do not hesitate to contact us with any questions.

Sincerely,

Jeremiah Posedel
MDPC Secretariat and Legal Counsel