Dockets Management
Food and Drug Administration
5630 Fishers Lane, Rm 1061
Rockville, MD 20852

September 22, 2021

Ref: Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities (Docket No. FDA-2021-N-0561)

Dear Sir/Madam:

This is to submit comments on the discussion paper referenced above, as requested by the Food and Drug Administration (FDA) through the Request for Comments issued in June 2021. This document is divided into four sections for ease of reading and reference.

I. Introduction of ACCE

Before providing information and comments, please allow me to introduce the American College of Clinical Engineering (ACCE) so you can understand our perspective on this subject. ACCE was founded in 1990 with the mission of:

i. To establish a standard of competence and to promote excellence in clinical engineering practice,
ii. To promote safe and effective application of science and technology in patient care,
iii. To define the body of knowledge on which the profession is based, and
iv. To represent the professional interests of clinical engineers.

Currently, ACCE has over 2,000 members in the United States who work in various segments of the medical device ecosystem, ranging from research and development, manufacturing, servicing, regulatory affairs, marketing, consulting, and education. While most of our members are at the manager or higher levels, many of them are still performing hands-on service on medical devices. Some of our members oversee >1,000 frontline service professionals, while others lead smaller teams. Finally, our membership is very diverse in terms of age, sex, race, professional experience, and educational background.

Since its foundation, ACCE has participated in every discussion with the FDA on the issue of servicing, particularly the 1997 ANPR (Docket No. 97N–0477), the 2016 PR (Docket No. FDA–2016–N–0436), and the 2019 PR (Docket No. FDA-2018-N-3741). ACCE was also invited to present at the Servicing Workshop held on December 10-11, 2018 and discuss at the Workshop help on October 27-28, 2016. ACCE also participated in the Cybersecurity Workshop held on January 29, 2019.

II. General Comments

ACCE applauds FDA's initiative in discussing cybersecurity issues as it pertains to the servicing of medical devices and seeking comments from stakeholders in the medical device ecosystem on its challenges and opportunities.

ACCE identifies cybersecurity as a growing concern and is affecting healthcare providers across the United States and the world. The COVID-19 pandemic has demonstrated that threat actors and attackers do not wait and are getting creative with ransomware, botnets, fileless malware, and other attack pathways. The COVID-19 pandemic also demonstrated the critical need to make devices available at all times for patient care and the effect service interruptions can have on care delivery and its safety and reliability.

Medical device cybersecurity management is a shared responsibility for stakeholders in this ecosystem and that includes OEMs, HDOs, OEM-affiliated multivendor services (MVSs), ISOs, and others affiliated with healthcare providers, regardless of the device ownership.

Above all, medical device cybersecurity risks impact patient care and effectiveness of care delivery increasing operational, financial, and data pressures on healthcare providers.

ACCE agrees with the FDA that "FDA is not suggesting that devices be secured to prevent non-OEM servicing when such servicing is technically feasible and appropriate." However, without strict monitoring from the FDA, "privileged access" could become an operational, financial, and data strain on all healthcare providers, including all service entities except for OEMs servicing the devices they produced. OEMs could decline service activities and resulted in increased device downtimes, device unavailability, and impacted clinical workflows and patient care.

ACCE strongly believes in FDA's efforts in strengthening cybersecurity practices and doing so with service activities. Our recommendations and answers to the FDA discussion questions will be presented in this written comment.

III. Answers to FDA Discussion Questions

ACCE has answered the discussion questions presented in the discussion paper instead of commenting on each of the four areas. Our answers to the questions presents the concerns in each of the four areas and avoids redundancy.

1. What are the cybersecurity challenges and opportunities associated with the servicing of medical devices?

   Two main challenges that servicers are facing in addressing cybersecurity concerns are:

   - Privileged Access: almost all cybersecurity activities performed on medical devices by ACCE members, including various service entities, require "privileged access" to the devices. Without this access, it is impossible to address cybersecurity risks and mitigate/manage them, so it is safe and reliable for patient care. Without this access, service entities are constrained and may need to adopt practices outside of OEM recommendations, which can lead to unsafe and out of specification devices, including delays in patient care delivery and unnecessary costs. ACCE strongly urges

the FDA to mandate OEMs to provide this "privileged access" to service entities so cybersecurity risks can be addressed in a timely and cost-effective manner.

- Legacy Devices: legacy devices comprise a large percentage of a healthcare provider's medical device inventory. A recent analysis demonstrated that at-least 28% of the devices are Windows-based, 30% are non-Windows based, and 42% are proprietary operating systems.[1] Out of the 28% that are Windows-based operating systems, at least 10% were found to be unsupported or legacy devices[1]. Service entities outside of the OEMs are severely strained to manage these legacy devices and often the only mitigation action is to replace or upgrade them, which leads to high expenses for the HDOs. ACCE strongly urges the FDA to foster negotiation between OEMs and HDOs to establish a mutually beneficial roadmap that manages the cybersecurity risks with legacy devices and gradual phase-out plan. In addition, an average medium sized HDO with 10% of legacy devices may need hundreds of millions of dollars in replacement cost. With less than 1% of total HDO expense allotted for service entities, this is a financial crisis waiting to happen.

2. Are the four areas identified in this discussion paper (privileged access, identification of cybersecurity vulnerabilities and incidents, prevention and mitigation of cybersecurity vulnerabilities, and product lifecycle challenges and opportunities) the correct cybersecurity priority issues to address in the servicing of medical devices? If not, which areas should be the focus?

   The four areas identified in this discussion paper identify issues that need to be addressed. However, this discussion needs to be inclusive of HDOs and service entities that are challenged with managing cybersecurity risks, that are outside of OEMs.

   Two particular cybersecurity priorities that need to be addressed for the HDO stakeholders are described below. While some may argue that this is not FDA or OEM's responsibility, these are expenses HDOs incur due to lack of cybersecurity controls designed into the medical devices:

   - Capital Expenses: if privileged access were to be strictly limited by OEMs, it is going to result in additional capital expenses for HDOs and other users of the devices. This includes:
     - Increased cost to buy and deploy new devices to compensate for the delay in servicing due to privileged access.
     - Shorter device life cycles, which means, faster replacement of the devices causing patient care delivery interruptions and capital spend.
   - Operational Expenses: if servicing with privileged access is the only option for HDOs to remediate cybersecurity risks, it is going to result in impractical cost increases for HDOs and likely result in overall increase in healthcare costs.

[1] Analysis of operating systems in medical devices by Asimily. Available at: https://www.asimily.com/podcasts

ACCE recommends that the FDA includes the American Hospital Association (AHA), Federation of American Hospitals (FAH), American Medical Association (AMA), American College of Healthcare Executives (ACHE), and Supply Chain trade associations to identify and address challenges around cybersecurity priority issues.

3. How can entities that service medical devices contribute to strengthening the cybersecurity of medical devices?

   ACCE's members come from variety of service backgrounds, not limited to HDOs, ISOs, OEMs, MVSs, software solution providers, security researchers, and others. Regardless of the who employs the service personnel, all service personnel contribute routinely to strengthening the cybersecurity of medical devices. Almost all service personnel perform activities that mitigate and manage cybersecurity risks, despite these activities being limited due to privileged access, lack of software updates, and other mitigating factors available from OEMs.

   ACCE's Cybersecurity Task Force raised numerous concerns throughout the COVID-19 pandemic where OEMs declined service, privileged access, software keys and even updates to critical cybersecurity risks. This severely constraints HDOs and other providers to provide timely care for patients and keep equipment uptime at much-needed times.

   ACCE strongly recommends that FDA engage in a workshop that brings together HDO and other providers to understand the challenges they experienced and how patient care was impacted due to the unavailability of OEM services and software keys/licenses (privileged access) to address cybersecurity risks, including unavailability of services amidst the COVID-19 pandemic when OEMs declined to send their service personnel for scheduled and unscheduled maintenance activities. This will demonstrate specific responsibilities and stakeholder commitment to strengthening cybersecurity, while managing surge needs amidst the COVID-19 pandemic.

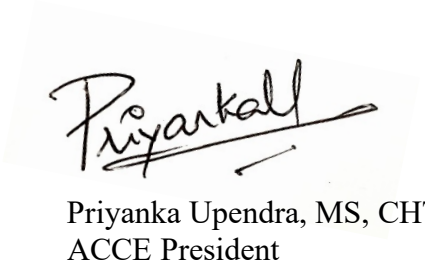
IV. Conclusions

ACCE applauds the FDA for its effort to strengthen cybersecurity and the opportunity to provide feedback and answer timely questions.

Medical device cybersecurity is a shared responsibility among all stakeholders in the medical device ecosystem and this includes OEMs, HDOs, ISOs, MVSs, and others. The challenges across this domain extend beyond servicing and are outlined in this written comment. Therefore, ACCE urges the FDA to broaden this discussion and engage all relevant stakeholders and their trade associations.

Finally, ACCE is grateful for the opportunity provided by the FDA to comment on this discussion paper and more importantly on this issue, which continues to be a challenge for its members. ACCE and its task force is committed to participating in future workshops, further discussions, and any assistance in this effort. Please feel free to contact me if you have any questions.

Very Sincerely,



Priyanka Upendra, MS, CHTM, AAMIF
ACCE President
president@accenet.org

Cc: William H. Maisel, MD (William.Maisel@fda.hhs.gov)
Joshua Silverstein, PhD (Joshua.Silverstein@fda.hhs.gov)
ACCE Board
ACCE Cybersecurity Task Force