American Hospital Association

800 10th Street, NW
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100 Phone
www.aha.org

May 24, 2018

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

RE: Docket Number FDA-2018-N-1315, Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health.

To the Dockets Management Staff:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to respond to the Food and Drug Administration's (FDA) Medical Device Safety Action Plan, particularly with regard to advancing medical device cybersecurity. **The AHA appreciates the FDA's focus on medical device security and encourages the agency to expedite its plan and act swiftly to provide greater oversight of medical device manufacturers with respect to the security of their products.**

Hospital and health system leaders recognize that data held by health care organizations is highly sensitive, as well as valuable, and are taking cybersecurity challenges extremely seriously. The vast majority of hospitals already are taking many important security steps to safeguard data while they continue to enhance their data protection capabilities (details on the steps hospitals are taking can be found at www.aha.org/cybersecurity). However, last year's global WannaCry ransomware attack underscored the cybersecurity risks hospitals and health systems face, including the extent to which medical devices are vulnerable and can create serious risks for the security of hospitals' overall information systems.

The Medical Device Safety Action Plan outlined four steps under consideration by the FDA:

- Consider new premarket authorities that would require manufacturers to build capability to update and patch device security into product design and provide a "Software Bill of Materials" that identifies the information technology solutions in a device so that end-users can better manage the devices;
- Update existing premarket guidance to better protect against moderate and major risks that could disrupt clinical operations and delay patient care;

- Consider new post-market authority to require manufacturers to adopt policies and procedures for coordinated disclosure of vulnerabilities when they are identified; and
- Explore the development of a CyberMed Safety (Expert) Analysis Board to be a public-private partnership to complement existing device vulnerability coordination and response activities and serve as a resource for device makers and FDA.

The AHA supports these steps, which would make important improvements to the FDA's oversight of medical device manufacturers with respect to the security of their products. We urge the FDA to move as quickly as possible to implement them and make public its timeline for the benefit of all stakeholders.

With regard to the coordinated disclosure of vulnerabilities, we urge the FDA to address the timeliness of those disclosures, and also to set expectations for manufacturers to provide timely information on patches and mitigating steps. Additionally, the FDA may want to consider creating a single repository of information for disclosures so that end-users can easily access it during times of crisis. Finally, we urge the FDA to outline how the agency itself will support manufacturers and end-users of devices during a large-scale attack.

With regard to the development of a CyberMed Safety (Expert) Analysis Board, we recommend that the FDA also consider including providers as a partner in its creation and deployment. They, too, stand to benefit from the Board's expertise on how to assess vulnerabilities, evaluate patient safety risks, assess proposed mitigations, and the other functions described in the safety plan.

While the FDA has released both pre- and post-market guidance to device manufacturers on how to secure systems, these manufacturers have yet to resolve concerns, particularly for the large number of legacy devices still in use. **Manufacturers must be held accountable to proactively minimize risk by building security into products by design, providing security tools to their end-users and updating and patching devices as new intelligence and threats emerge.** They share responsibility for safeguarding the confidentiality of patient data, maintaining data integrity and ensuring the continued availability and functionality of the device itself.

While no actions can completely eliminate cybersecurity risks from health care, swift action by the FDA to improve the security of medical devices will address a significant source of vulnerability. The AHA stands ready to serve as a resource to the agency as it implements these aspects of the Medical Device Safety Action Plan.

Thank you for your consideration of our comments. Please contact me if you have questions or feel free to have a member of your team contact Chantal Worzala, vice president of health information and policy operations, at cworzala@aha.org or (202) 626-2313.

Sincerely,

/s/
Ashley B. Thompson
Senior Vice President
Public Policy Analysis and Development