American Hospital Association

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

November 21, 2014

Submitted Electronically

Leslie Kux
Assistant Commissioner for Policy
Food and Drug Administration
5630 Fishers Lane, Room 1061
Rockville, MD 20852

Re: Request for Comments on Collaborative Approaches for Medical Device and Healthcare Cybersecurity [Docket No. FDA-2014-N-1286]

Dear Ms. Kux:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our 43,000 individual members, the American Hospital Association (AHA) appreciates the opportunity to comment on the Food and Drug Administration's (FDA) *Collaborative Approaches for Medical Device and Healthcare Cybersecurity*, which was published in the Federal Register on Sept. 23, 2014.

Hospitals take seriously their responsibility to protect their information systems from unauthorized access and malicious attacks. Health care is becoming more and more connected. This connectivity is yielding tremendous efficiencies and innovations. However, it also has introduced new types of vulnerability for inappropriate access to private information, and even criminal activity, that can put individuals and institutions at risk. As noted in the request for comment, and during the corresponding public workshop, hospitals increasingly are connecting medical devices to their information systems, presenting yet another avenue for bad actors to exploit vulnerabilities.

The AHA is pleased that the FDA is raising the issue of medical device cybersecurity and encourages the agency to continue taking steps to bring medical device security protections in line with state-of-the-art practice. Below please find our answers to the five questions posed by the agency in its request for comment.

If you have any questions, please contact Chantal Worzala, director of policy, at cworzala@aha.org or Lawrence Hughes, assistant general counsel, at lhughes@aha.org.

Sincerely,

/s/

Linda E. Fishman
Senior Vice President
Public Policy Analysis and Development

American Hospital Association (AHA)
Detailed Answers to Questions Posed in the Food and Drug Administration's (FDA)
Collaborative Approaches for Medical Device and Healthcare Cybersecurity

Question 1. Are stakeholders aware of the ''Framework for Improving Critical Infrastructure Cybersecurity''? If so, how might we adapt/translate the Framework to meet the medical device cybersecurity needs?

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," directed the National Institute of Standards and Technology (NIST) to develop the framework to "reduce cyber risk and help owners and operators of critical infrastructure identify, assess, and manage that risk." Hospitals are included in the Healthcare and Public Health [HPH] Critical Infrastructure Sector, one of 16 sectors identified in the executive order. The framework, accessible at http://www.nist.gov/cyberframework/, consists of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks. NIST does not have enforcement authority, and the framework is voluntary for the private sector, although it is mandatory for federal agencies. An organization can use the framework as a key part of a systematic process to identify, assess and manage cybersecurity risk.

The AHA has undertaken numerous efforts to raise hospitals' awareness of cybersecurity in general, and the NIST Framework in particular. For example, the AHA has developed cybersecurity guides for hospital and health system CEOs and trustees, and hosted numerous webinars, including one specifically devoted to the NIST Framework. We also have shared a summary outlining the NIST Framework with all of our member hospitals and health systems. All of these materials are posted to the AHA cybersecurity webpage at www.aha.org/cybersecurity, which also includes information on how to connect to federal and private-sector information-sharing activities.

Nevertheless, the resources in the NIST Framework can be challenging for health care providers, and particularly smaller providers, to access and use. **The AHA recommends that NIST and partner federal agencies make additional efforts to ensure that the guidance and standards are scalable to the smallest actors in critical infrastructure sectors, including physician offices and small rural hospitals.**

As critical infrastructure entities, hospitals and health systems must have the cooperation of all other entities that interact with their information systems, such as insurance companies, electronic health record (EHR) vendors and medical device manufacturers. All of these outside organizations also must engage in cybersecurity risk assessment and reduction activities, and the controls presented in the framework must flow down to their products. For example, medical device manufacturers will need to implement appropriate access controls, logging systems and vulnerability remediation tools. At the same time, device manufacturers need to develop security appropriate for the "least-resources" environment to which they market, such as the physician office, a small hospital or even a consumer at home. They cannot assume that the end-user will have a sophisticated security system with the capacity to implement high-level controls.

Question 2. How can we establish partnerships within the HPH Sector to quickly identify, analyze, communicate, and mitigate cyber threats and medical device security vulnerabilities?

The AHA recommends that the FDA hold device manufacturers accountable for cybersecurity, while also encouraging them to participate in the existing HPH activities to share information on cyber risk. Hospitals and health systems must consider the full spectrum of cyber threats, not just those involving medical devices. However, medical devices have been identified as key vulnerabilities and high-risk areas for the security of hospitals' overall information systems. The HPH sector cannot successfully protect against cyber risk unless all parts of the sector actively manage risk. Therefore, medical device security must be seen as both an issue to address on its own and as a component part of the overall landscape.

Medical device manufacturers must embrace their responsibility to proactively minimize risk and continue updating and patching devices as new intelligence and threats emerge. These obligations include safeguarding confidentiality of patient data, maintaining data integrity and assuring the continued availability of the device itself. The scope of devices to be considered should include both new devices and the large number of legacy devices still in use. The scope will continue to grow as innovation leads to new types of devices, potentially including those connected to mobile platforms.

Medical device manufacturers also must participate in existing information-sharing activities, such as the Healthcare and Public Health Sector Coordinating Council, the Healthcare and Public Health Information Sharing and Analysis Center (NH-ISAC), the Health Information Trust Alliance (HITRUST), InfraGard and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). These various public, private and joint forums allow participants to share the threats and vulnerabilities they observe, and learn how best to protect against emerging attacks. Given the interconnected nature of health care today, the AHA would discourage the formation of a separate, stand-alone information-sharing forum for the medical device community, although we recognize that separate activities within the medical device sector may be useful for technical conversations. Any cybersecurity discussions internal to the medical device community should be systematically brought to the larger, existing information sharing platforms.

Question 3. How might the stakeholder community create incentives to encourage sharing information about medical device cyber threats and vulnerabilities?

As end-users of health information technology (IT) products, communications services and medical devices, hospitals have very strong incentives to engage in protective activities. Any additional incentives contemplated for hospitals and health systems should include only positive incentives, such as reduced premiums for cybersecurity insurance.

From a statutory and regulatory perspective, hospitals face significant civil (and possibly criminal) penalties for data breaches that expose protected health information under the Health Information Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). The Medicare and Medicaid EHR Incentive Programs also place requirements on hospitals and other health care providers to adopt specific

security standards and take specific actions to ensure security. As trusted community institutions, hospitals also must guard their reputations. And, of course, if a cyber-event were to occur, it would result in significant financial and other costs. These significant incentives are leading hospitals to actively engage in managing their cyber risk. The attached data sheet provides information on cyber protections that hospitals already have in place.

As the regulator of medical devices, the FDA has a role to play in ensuring that risk is minimized by manufacturers and that they engage in information-sharing activities. The AHA applauds the agency's recent guidance on content of pre-market submissions for management of cybersecurity in devices. However, we urge the FDA also to address expectations of manufacturers for legacy devices. Many medical devices are designed for use over many years, and must be maintained for both the intended function and evolving cybersecurity threats. In looking at standards for cybersecurity, specifically, we urge the agency to consider both national and international standards, as well as the balance between creating assurances and promoting innovation. Vulnerabilities in a medical device can jeopardize a hospital's entire information system, with possible implications for patient safety as well as security of information. The agency also should urge medical device manufacturers to engage in cybersecurity information-sharing activities.

Question 4. What lessons learned, case studies, and best practices (from within and external to the sector) might incentivize innovation in medical device cybersecurity for the HPH Sector? What are the cybersecurity gaps from each stakeholder's perspective: Knowledge, leadership, process, technology, risk management, or others?

As the makers of a key component of modern health care, medical device manufacturers should embrace their role in assessing the applicability of the NIST Framework to their products, and use it as a springboard to make improvements in medical device security. As the end-users, hospitals and health systems spend significant resources to assess and modify device security. It would be helpful to hospitals and other end-users if manufacturers across the industry took a more structured, standardized approach for achieving security. At a minimum, all medical devices should include automated tools to track access and/or identify attempts at unauthorized access. Device manufacturers also may need to consider adopting "whitelisting" approaches, so that only approved processes can run on a device. Hospitals may need to consider whether devices should be segregated within a network.

Device manufacturers must be forthcoming about the vulnerabilities they identify in products, inform customers in a timely manner of all possible vulnerabilities and provide ongoing upgrades and support to improve security. Of course, information must be actionable to be useful – customers need to know how to take action to protect against a vulnerability. It is encouraging that device manufacturers are working with institutions such as the Mayo Clinic to learn about how their devices perform (or fail to perform) in real-world settings, as discussed at the recent FDA workshop.

Question 5. How do HPH stakeholders strike the balance between the need to share health information and the need to restrict access to it?

As the federal government continues to build out additional standards, information-sharing activities and other activities to promote security, it will be important to understand how they interact with the security rules already in place for health care, and avoid any contradictory or duplicative requirements.

Hospitals and health systems struggle daily with the delicate balance between sharing health information and ensuring its security. Cybersecurity involves much more than protecting patients' medical information and extends to all financial, personnel and other networked systems. Nevertheless, the HIPAA and HITECH requirements regarding protected health information form the regulatory backdrop for these considerations. For example, new structures to facilitate sharing information about medical device vulnerabilities must either be set up in a way that does not require sharing individual patient-level data, or provide a clear authorization to provide any essential patient-level data without violating HIPAA.

Hospitals Implementing Cybersecurity Measures

As hospitals increasingly use digital technology to gather, store and share patient information, they also must take steps to ensure data security. Results from the 2014 AHA Most Wired Survey show that the majority of hospitals are already taking many important security steps (see table below), while they continue to build out their capabilities.

Digital health will continue to evolve, and increasingly leverage secure connectivity for patients, physicians and other care providers. In response to both these technology shifts and the complex regulatory environment, best practices will continue to spread and change over time. Security is not just a technical issue, and many different steps need to be taken to ensure that hospital policies and staff training support information system security. Hospitals also must ready their response plans for those occasions when incidents arise.

Technical trends make clear that cybersecurity will be a growing issue for hospitals and their boards in the coming years. As a result, hospitals also will want to continue to build their capacity to keep information secure, identify threats and respond to incidents. The AHA has developed high-level resources for hospital leadership to help them navigate these issues, available at *www.aha.org/cybersecurity.*

Most Wired Survey Tracks Hospital Use of Important Cybersecurity Measures

Measure	Share of hospitals implementing measure:		
	More than 90%	More than 80%	More than 70%
Unique identification of system users	√		
Automatic logoff of system users	√		
Required use of strong passwords		√	
Passcodes for mobile devices	√		
Use of intrusion detection systems		√	
Encryption of wireless networks	√		
Encryption of laptops and/or workstations	√		
Encryption of removable storage media			√
Encryption of mobile devices			√
Remote data wiping of mobile devices		√	
At least annual risk analysis to identify compliance gaps and security vulnerabilities	√		
At least annual infrastructure security assessment		√	
Security incident event management			√

Note: The data presented are for all responding hospitals. For each measure, those recognized as Most Wired had higher levels of performance.

About Most Wired: The Most Wired survey is an annual benchmarking and recognition survey for hospital use of information systems. The 2014 Most Wired survey included data representing 1,901 hospitals, roughly 33 percent of all U.S. hospitals. The survey is conducted by Hospitals and Health Networks, in cooperation with the AHA and CHIME, and the next round will begin in January 2015. Learn more at *www.hhnmostwired.com.*