American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

June 24, 2022

The Honorable Bill Cassidy, M.D.
United States Senate
520 Hart Senate Office Building
Washington, DC 20510

The Honorable Tammy Baldwin
United States Senate
709 Hart Senate Office Building
Washington, DC 20510

Dear Senators Cassidy and Baldwin:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, 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) writes in support of the Protecting and Transforming Cyber Health Care (PATCH) Act (S.3983). AHA and its members are strongly committed to preparing for and preventing cyber-attacks

We are pleased to support this legislation to improve the security of medical devices, which can create cyber vulnerabilities and serious risks to the security and privacy of patient data along with vital medical technology used in care delivery. Cyber vulnerabilities in medical devices, often containing outdated legacy technology, have posed a significant cyber risk to hospitals. In 2017 the FBI reported that the North Korean WannaCry ransomware attack, which impacted hospitals around the globe, marked the first FBI observed cyberattack that affected medical device operability due to vulnerabilities present in those devices. Unfortunately, there have been scores of foreign-based ransomware attacks targeting U.S. hospitals since then, impacting medical device operability and risking patient safety.

This legislation would require medical device manufacturers to meet certain cybersecurity requirements when seeking approval for devices that are internet connected or include software. The provisions of the legislation, would make critical improvements to the Food and Drug Administration's (FDA) oversight of medical device manufacturers, including the requirement for medical device manufacturers to monitor and identify post-market vulnerabilities in a timely manner, develop a plan for coordinated vulnerability disclosure, provide lifetime cybersecurity support of the device and provide an accounting of all software contained in the device, including third party software. Vulnerabilities of third and fourth party software contained in medical devices continue to pose a significant risk to hospitals and health systems.

Manufacturers should be accountable for developing products with appropriate security controls, as well as updating devices as cyber threats continue to evolve. We also encourage the inclusion of a provision to clarify that FDA approval of devices would not be jeopardized as manufacturers provide these updates. Great strides have been made

by hospitals and health systems to defend provider networks, secure patient data, preserve health care delivery and, most importantly, protect patient safety.

We appreciate your leadership on this critical issue and look forward to working together to ensure the security of medical devices.

Sincerely,

/s/

Stacey Hughes
Executive Vice President