May 6, 2022

The Honorable Bill Cassidy, M.D.
U.S. Senate
520 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Tammy Baldwin
U.S. Senate
709 Hart Senate Office Building
Washington, D.C. 20510

Dear Senators Cassidy and Baldwin,

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) write today to express support for S. 3983, the "PATCH Act."

CHIME is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders. Consisting of more than 2,900 members in 60 countries, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. Launched by CHIME in 2014, AEHIS represents more than 950 healthcare security leaders and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members are among the nation's foremost health IT experts, including on the topics of cybersecurity, privacy and the security of patient and provider data and devices connecting to their networks.

Healthcare providers have long-held concerns that the policies medical device manufacturers must meet are simply sub-regulatory guidance documents that lack sufficient teeth to hold them truly accountable for ensuring cybersecurity is built into these devices. This is imperative as cybersecurity vulnerabilities pose a real risk to patient safety and many devices providers purchase arrive off the shelf and actually contain known vulnerabilities.

Under your legislation, manufacturers who submit for a premarket approval to the Food and Drug Administration (FDA) for a cyber device would be required to meet cyber requirements (with some exemptions). Included among these requirements would be mandating manufacturers have a plan to monitor, identify, and address post-market vulnerabilities in a timely manner and include a coordinated vulnerability disclosure. Moreover, manufacturers would also be required to have a plan in place to make updates and patches throughout lifecycle of a device. Failure to comply with these policies would result in civil monetary penalties.

Our members prioritize patient safety and safeguarding patient data. While some medical device manufactures have made strides around improving medical device security over the last few years as the FDA has increased their scrutiny of these practices, many medical devices still lack appropriate safeguards and do not contain adequate cyber protections. A long-standing concern of our members has been that the FDA guidance documents are stamped with the word "Contains Nonbinding Recommendations" which has been and continues to be interpreted by some manufacturers to mean that meeting cyber requirements are merely a suggestion. We know the FDA has state unequivocally that this is not the case, however, the reality is some

manufacturers continue to ignore this, or small vendors do not fully understand the requirements. Your legislation will go a long way to improving this situation by giving teeth to non-compliance.

We believe your legislation could be strengthened even further if the following provisions were added:

- Requiring manufacturers to disclose when outside/internet connections will be required and restricting their needs to specific IP addresses.
- In addition to requiring that the primary vendors disclose known vulnerabilities, disclosure of secondary and tertiary (etc.) vendors' vulnerabilities is also needed. Many primary vendors' products contain components and software from other vendors. One of our members cited a well-known healthcare robot used in hospitals across the country as having third-party vulnerabilities that caused it to try and communicate with Russia.
- Clarification around the definition of "cyber device" includes the need to address the capture, storage, and transmission of protected health information (PHI) as defined under the Health Insurance Portability and Accountability Act (HIPAA), something we recommend is included.
- Finally, we recommend the bill be amended to include a provision that explicitly allows manufacturers to update their software without invalidating their FDA approval, something FDA has made clear is not only permissible but encouraged. Nonetheless, manufacturers continue to refuse to patch software hide behind excuses that doing so would risk their FDA approval.

We appreciate the work you are doing to improve safety of medical devices by imposing these mandates on medical device manufacturers and establishing greater oversight and we would be happy to discuss with your staff the additional ideas we have for strengthening the legislation even further.

Should you have any questions about our position or if more information is needed, please contact Cassie Leonard, Director of Congressional Affairs, at cleonard@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME

Sri Bharadwaj, MS, FCGMA, FHIMSS, CPHIMS, CISSP, CLSSBB, PMP, CHCIO
Chief Operations and Information Officer
Longevity Health