December 21, 2021

The Honorable Diana DeGette
United States House of Representatives
2111 House Office Building
Washington, DC 20515

The Honorable Fred Upton
United States House of Representatives
2183 House Office Building
Washington, DC 20515

Dear Congresswoman DeGette and Congressman Upton,

The College of Healthcare Information Management Executives (CHIME) is pleased to respond to your request for input on H.R. 6000, the Cures 2.0 Act.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With over 5,000 members, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate for the effective use of information management to improve the health and healthcare in the communities they serve.

CHIME applauds your commitment to bipartisanship and willingness to engage stakeholders as you pursue policy changes. As Cures 2.0 moves through the legislative process, we ask that you consider the following health IT-related recommendations that will strengthen the historic Cures Act legislation signed into law in 2016 and further our shared vision of an interoperable healthcare system.

Spurring Greater Interoperability:

- **Health Information Exchange.** To better incentivize participation in a health information exchange (HIE) or national health information network (HIN) such as CommonWell and CareQuality, Congress should reduce the cost burden associated with joining these methods of health information exchange that are crucial for attaining a national interoperable healthcare network. This is particularly important for small and rural providers and could be accomplished through reimbursement programs or vendor contributions.
- **National Standard for Data Exchange.** A national definitive standard for data exchange is needed to better support the exchange of electronic health information pertaining to public health data reporting, e-prescribing and to facilitate cross-state Prescription Drug Monitoring Program (PDMP) exchange. Currently no cross-state

standard exists and as such, many reporting programs within states are not accessible outside of that state.

- **Supporting Interoperability Across the Care Continuum.** We would also emphasize the impact of deficiencies in technology adoption across the care continuum. While the Meaningful Use Incentive program furthered the adoption of electronic health records by most physicians, hospitals, and critical access hospitals (CAHs), other care settings, such as long-term post-acute care (LTPAC) providers and behavioral health providers, were not included. These provider types often do not have the resources to implement or maximize the use of EHR technology. For this reason, CHIME believes funding is needed for these providers to purchase and deploy certified EHRs as mature as the one's hospitals have and to participate in health information exchanges. In addition, it is our recommendation that the Cures Act be amended to add a seat to the HITAC committee[1] nominated by the Government Accountability Office (GAO) designated specifically for LTPAC providers to bring greater awareness to data sharing challenges across the care continuum and patient needs as they transition to LTPAC settings of care. Finally, we recommend that the HITAC committee's annual report feature a section focused on the state of interoperability across the entire care continuum, including in LTPAC settings.
- **Reexamining the Definition of an EHR.** Given that patients are now able to manage their own health on platforms such as smartphones and tablets, and soon providers will be increasingly interacting with EHR type systems via these means, we recommend broadening the understanding of what is a EHR to include these new forms of electronic health record technology.

Public Health Infrastructure: We are grateful to Congress for providing nearly $1 billion to date for the Centers for Disease Control & Prevention's Data Modernization Initiative through annual and supplemental appropriations. However, sustained, annual investments are needed over the next decade to complete this foundational investment to ensure we are investing in public health systems and infrastructure that will keep pace with evolving technology.

Privacy: Among our members, concerns continue to mount as healthcare data is increasingly exchanged both among and outside non-traditional healthcare settings, and as consumers become active managers of their health information. We are particularly concerned that as more patients share their healthcare data with third parties, that data could be mishandled, including being sold to data aggregators and used to discriminate against consumers in the future. As a result, we strongly recommend Congress provide greater oversight of non-regulated third-party applications that handle PHI (which are not presently governed by HIPAA), including by reviewing and revising the Federal Trade Commission's (FTC) already in place – but rarely utilized – breach notification requirements, something the agency itself has indicated they plan to do further. However, it is clear the FTC would need additional funding in order to robustly commit to these efforts. We would also like Congress to consider facilitating a pathway for third-party applications to be certified or at minimum demonstrate trustworthiness. This would be a positive first step as Congress deliberates the creation of a comprehensive national data privacy law.

Security: As we increase interoperability, additional threats to data integrity will arise. Without proper safeguards, the safe and secure transmission of sensitive data will continue to be a challenge and will hinder efforts to provide positive care outcomes. As a result, it is

vital that Congress and HHS identify a pathway for ensuring providers do not unduly shoulder the burden of protecting PHI in situations outside their control as cybersecurity is a shared responsibility. For instance, developers of software who are aware of a vulnerability, but fail to patch or notify customers of that vulnerability, should be held accountable if the known but unpatched vulnerability leads to a breach. Unlike HIPAA breaches where there are significant penalties for providers, there are few for medical device manufacturers. Similarly, developers who knowingly develop their technology through labor practices known to lead to crucial coding mistakes and the creation of software vulnerabilities, should shoulder the burden for consequence if a breach were to occur, not the consumer of the technology, such as a provider, who would have no ability to know about the vulnerability or protect themselves from it. FDA specifically requested additional authority in their FY21 budget to ensure medical devices with known vulnerabilities are not approved[2].

We hope our comments to Cures 2.0 are useful and look forward to a continued dialogue regarding legislative solutions for improving healthcare for patients through the use of technology. Should you have any questions or if we can be of assistance, please contact Cassie Leonard, Director of Congressional Affairs, at cleonard@chimecentral.org.

Sincerely,

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

[1] Established under Section 3002 of the Cures Act.
[2] https://www.fda.gov/media/135078/download (page 41)