September 23, 2019

The Honorable Lamar Alexander
Chair
Senate Committee on Health, Education, Labor and Pensions
455 Dirksen Senate Office Building
Washington, DC 20515

The Honorable Patty Murray
Ranking Member
Senate Committee on Health, Education, Labor and Pensions
154 Russell Senate Office Building
Washington, DC 20515

Dear Chairman Alexander and Ranking Member Murray:

The undersigned organizations represent the nation's clinicians, hospitals, health systems and foremost experts in health informatics and health information management. We write today to encourage the Committee's continued oversight to ensure that the 21st Century Cures Act (Cures) is implemented in a manner that best meets the needs of patients and those who deliver their care. We are concerned that specific provisions of the Office of the National Coordinator for Health Information Technology's (ONC's) recent proposed rule jeopardizes important goals to foster a healthcare system that is interoperable, patient-engaged, and reduces burdens for those delivering care.

We acknowledge and support proposed provisions that will help advance the nation's ability to leverage health information technology (health IT) in the care delivery process, such as proposals related to application programming interface (API) standards, electronic health record (EHR) certification, and EHR vendor business practices and behaviors. We are also supportive of the rule's attention to the issue of improving patient matching, a critical factor for achieving effective interoperability, improved patient safety, and enhanced care coordination.

While we are pleased the Administration is working to operationalize several requirements in Cures that seek to improve information sharing and patient care through use of APIs, at the same time it is imperative that policies be put in place to prevent inappropriate disclosures to third-parties and resultant harm to patients. We offer the following recommendations aimed at furthering the objectives of Cures, while ensuring that the final regulation does not unreasonably increase provider burden or hinder patient care.

Specifically, we recommend that the regulations implementing Cures incorporate the following:

- **Additional rulemaking prior to finalization:** To ensure a sufficient level of industry review and to appropriately respond to stakeholder feedback, ONC should issue a supplemental rulemaking to address outstanding questions and concerns.
- **Enhanced privacy and security:** The proposed rule does not sufficiently address Cures' directives to protect patient data privacy and ensure health IT security. Further, it is imperative that the Committee continue its oversight of privacy and security issues that fall outside of the Health Insurance Portability and Accountability Act (HIPAA) regulatory framework.
- **Appropriate implementation timelines:** ONC should establish reasonable timelines for any required use of certified health IT (CEHRT). Providers must be given sufficient time to deploy and test these systems, which must take into account competing regulatory mandates.
- **Revised enforcement:** The U,S, Department of Health and Human Services should use discretion in its initial enforcement of the data blocking provisions of the regulation, prioritizing education and corrective action plans over monetary penalties.

Please see the enclosed attachment, which describes these recommendations in more detail.

We appreciate the Committee's dedication to improving the nation's healthcare through deployment of effective health IT and for its ongoing commitment to provide oversight during the implementation of Cures. Our organizations thank you for the opportunity to bring these important issues to your attention and look forward to working collaboratively to ensure the goals of this landmark legislation are met. Please contact Leslie Krigstein, Vice President of Congressional Affairs at CHIME, lkrigstein@chimecentral.org, with any questions you may have.

Sincerely,

American Health Information Management Association (AHIMA)
American Medical Association (AMA)
American Medical Informatics Association (AMIA)
College of Healthcare Information Management Executives (CHIME)
Federation of American Hospitals (FAH)
Medical Group Management Association (MGMA)
Premier Inc.

Recommendations Regarding ONC Interoperability Rule

Additional Stakeholder Input and Rulemaking

ONC should issue a Supplemental Notice of Proposed Rulemaking (SNPRM) and seek further input from impacted stakeholders on issues including:

- Part 171 of the proposed rule contains the proposed information blocking exceptions, which are both complex and confusing.
- The rule proposes to define electronic health information (EHI), which is not defined in Cures. Due to the breadth of the proposed EHI definition, providers will need to use the currently ill-defined information blocking exceptions regularly, creating tremendous administrative burden as well as requiring significant legal assistance to navigate. ONC should modify the information blocking proposal to ensure that the requirements and exceptions are well-defined and understandable, and clinicians, hospitals, and health information professionals are not inappropriately penalized if they are unable to provide a patient's entire EHI through an API.

ONC should name a new Edition of CEHRT.

- ONC has proposed significant modifications to CEHRT. ONC should designate a new '2020 Edition,' rather than update the 2015 base EHR definition. As physicians and hospitals just adopted 2015 CEHRT this year, renaming the certification edition will provide clarity to all parties during future contracting and implementation processes.

Privacy and Security

- The use of APIs and third-party applications has the potential to improve patient and provider access to needed health information. It also brings us into uncharted territory as patients leave the protections of HIPAA behind. We support patients using apps to access their information; however, there is building concern that data will be commoditized by app developers and other third parties and used in ways not intended by patients.

- Certified APIs should include mechanisms to strengthen patients' control over their data – including privacy notices, transparency statements (including statements of whether data will be disclosed or sold) and adherence to industry-recognized best practices. This basic level of transparency is critical to strengthening patients' trust in an increasingly digital healthcare system.

- As more sensitive data is exchanged, CEHRT data segmentation capability should be prioritized. Standards and functionalities that enable data segmentation, tagging and privacy labeling are critical to ensuring the privacy of patient data. Segmentation of patient data will also be critical as we transition to a health information exchange trust framework and as the nation seeks to leverage health IT in addressing the opioid addiction crisis.

- As there are no security guidelines for vendors or providers as they on-board third-party apps onto their systems, ONC should develop a pathway to address security concerns in APIs and apps in coordination with impacted stakeholders. For example, API technology suppliers should be required to conduct surveillance and mitigate threats and vulnerabilities that could be introduced to an information system to which the API could connect.

- Multiple federal agencies have jurisdiction over the privacy and security of patient and consumer information, including the HHS Office for Civil Rights, the Federal Trade Commission, the Centers for Medicare & Medicaid Services (CMS) and ONC. We recommend the federal government adopt a holistic and coordinated approach to addressing the access, exchange and use of health information by third parties not governed by HIPAA, including the sale and commoditization of data not intended by patients.

- Additional requirements are needed to mitigate security concerns that arise with the on-boarding of third-party apps onto clinician and other providers' systems. Failure to do so could introduce significant cybersecurity threats to our healthcare system. Multiple stakeholders, including HHS' own cybersecurity advisory group, have raised these concerns.

Implementation Timelines

- Final regulations need to establish reasonable timelines for development and deployment of the next CEHRT edition. Further, HHS agencies – such as CMS – should also establish reasonable implementation timelines for clinicians and other providers required to use any new CEHRT edition in federal health IT and/or quality reporting programs.

- Implementation timelines should take into account the time necessary to operationalize the final rule once the above-recommended SNPRM is finalized.

- In considering appropriate timelines, ONC should coordinate with CMS and other applicable agencies to account for overlapping federal mandates like appropriate use criteria.

Information Blocking Enforcement (Discretion/Education)

- Given the complexity of the new policies around the information blocking exceptions for the clinician, hospital, and health information professional communities, ONC should provide examples of actions that would satisfy the information blocking exception requirements before the effective date of the information blocking final rule.

- HHS should use discretion in its initial enforcement, prioritizing education and corrective action over monetary penalties. We assert that prioritizing education will be more effective over the long-term in ensuring clinicians, hospitals and health information professionals are in compliance as they will better understand the regulatory requirements.