CHIME
College of Healthcare
Information Management Executives

Statement of the College of Healthcare Information Management Executives

House Committee on Energy and Commerce
Subcommittee on Health

Hearing on “Implementing the 21st Century Cures Act: An Update from the
Office of the National Coordinator”

2322 Rayburn

December 11, 2018

The College of Healthcare Information Management Executives (CHIME) welcomes the opportunity to submit a statement for the record for the December 11, 2018, hearing entitled, “Implementing the 21st Century Cures Act: An Update from the Office of the National Coordinator.” We appreciate the Committee’s leadership and continued oversight of the landmark 21st Century Cures Act.

CHIME represents more than 2,800 chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders at hospitals, clinics and other health organizations nationwide. CHIME members are responsible for the selection and implementation of clinical and business systems that are facilitating healthcare transformation through technology.

Technology adoption and robust data sharing are vital to enhancing the quality of care and efficiency of the nation’s healthcare system. Our members have extensive experience implementing technology that must interoperate with dozens of independent systems, ranging from diagnostic imaging and biomedical devices to financial and remote access systems. The passage and ongoing implementation of the 21st Century Cures Act presents policymakers and the industry with the opportunity to leverage the potential of health information technology to improve patient outcomes and accelerate access to lifesaving treatments.

Since enactment of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), the healthcare industry has made a significant shift in the way technology is used to treat and engage with patients. The myriad of provisions included in the 21st Century Cures Act such as reducing administrative burdens resulting from health IT, the Trusted Exchange Framework and Common Agreement, the EHR Reporting Program, the Health IT Advisory Committee (HITAC), the definition of what does not constitute information blocking and reports on patient access and patient matching will prove to have significant impacts on the health IT and healthcare delivery ecosystem in the future.

Administrative Burden
Policies ensure providers have access to technology necessary to facilitate their success in new payment models and drive care improvements for patients while ensuring the Administration pursues reasonable policies that will reduce provider burden, facilitate greater care coordination, and direct the maximum amount of attention on the care delivered to patients. A focus on improved outcomes (rather than process measures), facilitated by interoperability, will position providers for success in new payment programs while enabling the delivery of better care to patients.

Technical innovation must flourish but it is also important to keep in mind the importance of fostering the connection between patients and their clinicians. HHS must be mindful of keeping patients and caregivers connected to their providers so technology can be used to deliver better care, not detract from patient care. For instance, the Promoting Interoperability program has unwittingly incentivized clinicians to spend less time with their patients and more time in front of their computer screens. If innovations cause the distance between clinicians and their patients to grow, technology may be perceived as a barrier rather than a solution.

On November 20, 2018, the Office of the National Coordinator for Health IT (ONC,) along with the Centers for Medicare and Medicaid Services (CMS,) published the draft “Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs” as requested by the 21st Century Cures Act. This strategy articulates the Administration’s desire to reduce some of the regulatory and administrative burden that clinicians shoulder resulting from health IT rules and regulations. The inclusion of recommendations pertaining to prescription drug monitoring programs (PDMPs) and electronic prescribing of controlled substances (EPCS) are timely and welcomed as the nation grapples with how to leverage technology solutions to curb the opioid epidemic.

Trusted Exchange Framework and Common Agreement
ONC issued a draft of the Trusted Exchange Framework and Common Agreement (TEFCA) on January 5, 2018, with an additional opportunity to comment expected imminently. In the January draft, it was clear ONC’s intent as they crafted the TEFCA was to build from existing work already underway aimed at speeding interoperability. However, the draft agreement would create an entirely new national exchange network and it is not entirely clear how this will impact existing agreements, but it does appear to require a substantial amount of change processes. We recommend that ONC work collaboratively with the National Institute of Technology (NIST) as required under 21st Century Cures Act to pilot test TEFCA.

TEFCA is intended to advance interoperability across the healthcare continuum. Some provider segments, including but not limited to those delivering post-acute care (e.g., skilled nursing facilities, home health agencies) and behavioral health, were not included in prior programs that incentivized transition to electronic health records (EHRs). These segments of the healthcare sector continue to lag acute care providers in EHR utilization and in certified EHR technology (CEHRT) adoption. If we are to speed interoperability, all sectors of the healthcare system where patients receive care must be able to exchange data. Population health management and value-based payment implementation for an aging population and other populations for whom healthcare needs can be more complex, will face continued hurdles until post-acute care and other providers across the healthcare ecosystem reach health IT sophistication levels comparable to those of acute care. More attention to this facet of the interoperability conversation is warranted and requires ONC to elaborate on their vision for including more provider types. Rather than creating more hard mandates, collaborative solutions like pilot projects through the Center for Medicare and Medicaid Innovation (CMMI) have merit.

The intrinsic value of interoperability is undeniable, but providers have concerns about being able to put into practice what was outlined under the draft TEFCA. Therefore, each CIO will find him or herself in the spot of determining whether participation makes sense for his or her organization. The feasibility of revising all data exchange agreements on such a tight timeline, as proposed, is problematic. The complexity and aggressive timeframes could discourage some organizations from participating in TEFCA, at least initially. Also, the critical mass of TEFCA participation necessary for benefit to outweigh burden for most participants has not been discussed nor has ONC shared any projections for TEFCA uptake.

The 21st Century Cures Act indeed directs ONC to define interoperability to mean that information be exchanged without "special effort on the part of the user." The law also calls for enhanced certification requirements to accommodate this. The draft Framework did not address this topic, and it appears that this effort will be left to EHR vendors.

The TEFCA draft clearly stipulates that individual choices about access to and sharing of their data be provided at no cost and be respected. It appears that ONC anticipates that consent management will be managed at the Health Information Network (HIN) level, but few details are provided. The process of verifying consent and the maintenance of individual consent choice records in a nationwide data exchange environment offers considerable challenges. The forthcoming TEFCA draft should address Qualified Health Information Network (QHIN) involvement, Recognized Coordinating Entity (RCE) monitoring, and ONC oversight of data-sharing consent. The frequency with which consent choices must be updated should also be addressed by ONC to balance currency, accuracy, and administrative burden. Boundaries and approaches for handling of the complexity superimposed by varying state privacy laws and regulations deserve full consideration. We recommend ONC clearly address how they anticipate consent to be managed under TEFCA.

Further, the consequences to an organization of not participating are unclear; for example, could choosing not to participate be construed as data blocking? ONC must clarify how they envision the interface between TEFCA participation and data blocking regulations during the comment period on the data blocking rule. Also, we are unclear about what the impact to providers will be if some HIEs in their region join TEFCA while others do not. ONC must clarify this as well.

EHR Reporting Program

ONC and Congress have recognized the need for more transparency for EHR end-users, through the establishment of the EHR Reporting Program. ONC published a Request for Information (RFI) on the reporting program on August 24, 2018, and many stakeholders, including CHIME, suggested that what was proposed in the RFI is too onerous for the providers as purchasers of these systems even if it helps them evaluate products.

Vendors should be developing products which are inherently more usable and interoperable and the burden for ensuring this occurs should fall less on providers and occur prior to these systems even reaching the hands of clinicians. As ONC monitors vendors' interoperability capabilities they should consider establishing benchmarks and leverage existing industry sources to monitor progress.

Information Blocking

Effective April 1, 2016, the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) required both clinicians and hospitals to attest they are not “data blockers.” Accordingly, in this rule CMS calls on providers to demonstrate that they have not knowingly and willfully taken action (such as disabling functionality) to limit or restrict the compatibility or interoperability of CEHRT. Congress and the Administration are to be commended for their interest in combatting information blocking practices within the healthcare industry. There is no place for data blocking in healthcare and patients have a right to timely and secure access to their health information.

Unlike the current CMS information blocking attestation mandate, forthcoming rulemaking from the ONC and Office of the Inspector General (OIG), must recognize the limitations of current technology, regulatory barriers, and challenges some resource-strapped providers face. In terms of limiting or restricting the compatibility or interoperability of CEHRT, a note of caution must be heeded relative to the legal complexity that can ensue depending on how “not information blocking” is defined. Technology, social, economic and community factors must all be accounted for and meticulously evaluated when determining what constitutes “information blocking.” The cost of joining HIEs, interface fees and application programming interface development costs must be factored into the forthcoming rulemaking.

Robust information exchange and nationwide interoperability can flourish only once we can confidently identify a patient across providers, locations and vendors; however, that is not happening today. The importance of a coordinated national approach to linking patients to their healthcare data must be underscored. Ensuring that patients are positively identified and matched to their records is a linchpin to increasing interoperability and improving the quality and safety of patient care, especially in a highly digitized environment. When clear, enforceable standards are in play and patients can be safely and securely matched to their data to facilitate exchange, acts of blatant information blocking will become apparent.

Standards-based Interoperability

Among the charges of the Health IT Advisory Committee (HITAC) created by the 21st Century Cures Act is to focus on standards to facilitate interoperability. While a focus on data standards may seem overly simplistic, a more defined technical infrastructure is needed to catalyze innovations in digital health, now just as much as when the 21st Century Cures Act was enacted. Improved data standards will help ensure the data exchanged is valuable and useful to the receiving party. Our members feel that without this, we are destined to repeat mistakes by hoping the mere exchange of data will indeed result in improved outcomes. Without the ability for disparate systems to recognize and successfully use data, we are simply moving data, and in a very difficult and expensive way. For example, the current attempts by third-party developers to force electronic health record vendors to create one-off, custom Fast Healthcare Interoperability Resources (FHIR) interfaces, rather than implementing standardized FHIR interfaces is only adding to the difficulty and cost of interoperability – not improving it. To cure what ails this, a single set of named standards must be used by all parties.

Through the passage of the 21st Century Cures Act[1] Congress declared their interest in an interoperable health IT infrastructure. We recognize the work underway at ONC to tackle these challenges, nonetheless barriers remain and maintaining the status quo will stifle future progress. It’s imperative that ONC continue to leverage relationships with the private sector to capitalize on the progress made to date across the industry. Standards-based interoperability

[1] The 21st Century Cures Act (HR 34), 114th Congress. https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf

should be a top priority for ONC. Understanding how the lack of ubiquitous interoperability and meaningful data exchange is impeding care delivery and making necessary policy recommendations must be a priority as they promulgate TEFCA, as well as forthcoming rulemaking pertaining to information blocking. The Committee should direct ONC to ensure that the instruction to focus on standards and implementation specifications included in the statute is executed.

Patient Matching Report

Today patients and care providers are missing opportunities to improve people's health and welfare when data about care or health status is not easily available. The concept of a longitudinal healthcare record, which necessitates interoperability, should reflect the patient's experience across episodes of care, payers, geographic locations and stages of life. It should consist of provider-, payer- and patient-generated data, and be accessible to all members of an individual's care team, including the patient, in a single location, as an invaluable resource in care coordination and for public health purposes. Without a standard patient identification solution, the creation of an accurate longitudinal care record is simply not feasible.

Congress acknowledged the lack of a national solution to identifying patient is an interoperability and patient safety issue in the 21st Century Cures Act. Congress called on the Government Accountability Officer (GAO) to review policies and activities at ONC and other relevant stakeholders to ensure appropriate patient matching to protect patient privacy and security and ongoing efforts related to those policies and activities within two years of enactment. Further, Congress requested GAO to examine if ONC could improve patient matching by taking additional steps leveraging their current authorities. The report is forthcoming; however, ONC must continue to evaluate ways to improve patient identification and matching in the absence of a national patient identifier.

Application Programming Interfaces (APIs)

Cybersecurity attacks are highly disruptive and can be crippling to healthcare entities, as illustrated by the WannaCry and Petya ransomware attacks in 2017. The attacks impacted more than a dozen hospitals and countless other entities spanning the globe, reaching a reported 150 countries. Healthcare is deemed a critical infrastructure by the Department of Homeland Security (DHS) and as such, patient safety and patient data should be viewed as a public good; protecting those things should be a national priority.

Concerns remain with privacy and security of patient information with the use of application programming interfaces. Cybersecurity threats and emerging challenges associated with the use of APIs pose real concerns and our members continue to worry about the release of data to third parties at the request of patients without their clear understanding of how their data could be used. Recent consumer data breaches rooted in API weaknesses raise security concerns for protecting healthcare data.

As payment and delivery system reforms propel us towards greater connectivity, new vulnerabilities have arisen. Without proper safeguards, the safe and secure transmission of sensitive data will continue to be a challenge and will hinder efforts to care outcomes. We must ensure the implementation of stringent privacy and security standards.

As the Committee monitors the implementation of the 21st Century Cures Act, we urge Members to ensure that a standards-driven infrastructure anchored by a robust national patient matching strategy remains a priority as outlined in the statute.