Statement of the College of Healthcare Information Management Executives

House Committee on Energy and Commerce
Subcommittee on Health

Hearing on "Examining Barriers to Expanding Innovative, Value-Based Care in Medicare"

2322 Rayburn

September 13, 2018

The College of Healthcare Information Management Executives (CHIME) welcomes the opportunity to submit a statement for the record for the September 13, 2018 hearing entitled, "Examining Barriers to Expanding Innovative, Value-Based Care in Medicare." We appreciate the Committee's leadership and continued interest in the transformation of Medicare to better meet patient needs by leveraging technology.

CHIME represents more than 2,700 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 experience implementing technology that must interoperate with dozens of independent systems, ranging from diagnostic imaging and biomedical devices to financial and remote access systems. Several converging factors, including the passage and ongoing implementation of the 21st Century Cures Act, present policymakers with a unique opportunity to pursue and implement policies to bolster the digital infrastructure that will play a pivotal role in transforming care delivery.

Leveraging Technology to Modernize Healthcare

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 prolific adoption of electronic health records (EHRs) and other health IT resources by clinicians and patients will pay dividends as the nation's health system transitions to value-base care.

The transition away from fee-for-service reimbursement is not to be understated. Technical challenges and opportunities associated with generating reliable performance data to determine reimbursement will be a challenge with existing technology. For providers to be successful in new payment models, including those facilitated by the Medicare Access and CHIP Reauthorization Act (MACRA), a robust digital health infrastructure will be key. But, it is not enough to have data – there is already a prolific amount of data generated by our healthcare

system. The data must be able to be harnessed for the purposes of informing and bettering patient care. To ensure providers can leverage the data needed to enable a value-based, outcomes-driven care environment, the Committee should consider actions to:

1. Foster interoperability.
2. Reduce the burden of quality measure reporting for providers.
3. Enable innovation in healthcare technology.
4. Enhance the cybersecurity posture of healthcare providers.

Promoting Interoperability

Improving the quality of care and lowering costs will be contingent on the free flow of patient data across care settings, a must for delivery system reform. Unfortunately, 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. Notably, robust information exchange and nationwide interoperability can flourish only once we can confidently identify a patient across providers, locations and vendors.

Patient Identification for Interoperability
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 FY17 Omnibus Committee Report[1]. Congress then went on to clarify that the Office of the National Coordinator for Health IT (ONC) and the Centers for Medicare and Medicaid Services (CMS) can provide technical assistance to private-sector patient identification efforts. Efficiencies in care coordination, as intended by Congress in the HITECH Act, would be enhanced by a national strategy for patient identification. Congress could promote private-sector led solutions by encouraging CMS' Center for Medicare and Medicaid Innovation (CMMI) to include criteria that advances private sector-led solutions which facilitate unique patient identification or projects focused on this intended outcome.

Standards-based Interoperability
There is great potential to improve patient care and reduce healthcare costs through care coordination in an interoperable healthcare ecosystem. While a focus on data standards may seem overly simplistic, a more defined technical infrastructure is needed to catalyze innovations in digital health. 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 FHIR interfaces,

[1] Committee Report, H.R.244, Consolidated Appropriations Act 2017 (115th Congress) https://www.congress.gov/114/crpt/hrpt699/CRPT-114hrpt699.pdf

rather than implementing standardized FHIR interfaces is only adding to the difficulty and cost of interoperability – not improving it. To cure what ails this is a single set of named standards must be used by all parties.

The 21st Century Cures Act[2] declared Congress' 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 should thus 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 the Trust Exchange Framework and Common Agreement (TEFCA), as well as forthcoming rulemaking pertaining to information blocking. The Committee should direct ONC to ensure that the directive to focus on standards and implementation specifications included in the statute is executed.

Navigating Privacy and Consent Laws
The exchange of data among providers in various locations and settings will require the harmonization of state and federal privacy laws. As an example, consent policy varies by jurisdiction and personal health information (PHI) type, and similar to most privacy policies, there is no national patient consent policy. CHIME calls on Congress to lead an open dialogue to help states align privacy and consent policies that enable cross border exchange of health information in a secure manner; this should include re-examining certain provisions of Health Insurance Portability and Accountability Act (HIPAA) and 42 CFR Part 2 to further align patient consent policies around release of mental health and substance abuse data.

Healthcare organizations dedicate highly valuable resources to navigating these complexities to demonstrate compliance with its regulators and to meet patient demands. If a streamlined regulatory framework were in place, these resources could be better leveraged. Instead the patchwork of laws creates a burdensome environment which is costly and time-consuming to meet and detracts from, rather than supports, patient care. Congress should pursue legislation that harmonizes other privacy, security and information risk management requirements to eliminate the complex patchwork of regulations across industries and state lines. This effort should include a robust dialogue about patient privacy and consent laws, especially as they relate to sensitive health conditions. CHIME supported the Overdose Prevention and Patient Safety Act (H.R. 6082), which would remove an outdated regulatory barrier to allow providers to have access to the full medical history of patients suffering from substance use disorders.

Improving Quality Outcomes

The future of value-based reimbursement is contingent on the ability to accurately evaluate and continuously improve performance. Congress should prioritize a unified strategy for measuring, capturing and communicating quality in healthcare. Efforts have been underway since before the passage of HITECH to devise quality indicators that can be electronically captured in normal clinical workflow, yet organizations still must deploy sizable staffs for manual abstracting as electronically generated measures are often inaccurate and unreliable.

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

Currently, providers are required to report clinical quality measures (CQMs) to several public and private entities. Individual healthcare delivery organizations submit more than 20 reports across federal, state and private sector programs for various CQMs each month. Hours of work and expertise are required to comply with these reporting demands and such burdens are exacerbated by a lack of technical harmonization. Even when the same CQMs are used among different programs, they tend to require different technical specifications or values to be reported with different thresholds.

Efforts to reduce provider burden by streamlining reporting redundancies must be a priority and requiring data collection and submission on measures that do not advance patient care must cease. Access to real-time, actionable data will be critical for success in the Merit-based Incentive Payment System (MIPS) and alternative payment models (APMs). The Meaningful Measures initiative underway at the Centers for Medicare and Medicaid Services (CMS) appears to share the goal of eliminating duplicative quality measures and refocus on those that are focused on outcomes, thus reducing reporting requirements which in turn would decrease healthcare costs and allow clinicians to focus more attention on patient care.

Enabling Innovation in Healthcare Technology

A great deal of innovation is underway to develop population health tools and other new technologies that will be critical for advancing provider success in APMs. CMS must avoid a heavy-handed approach to determining what technologies providers must use. Further, the Department of Health and Human Services (HHS), more specifically CMS in coordination with ONC, should take an approach that allows innovation to continue to flourish rather than prematurely trying to certify these innovative technologies.

As the Committee monitors the implementation and administration of Medicare payment policies and programs, we urge members to ensure providers have access to technology necessary to facilitate their success in new payment models and drive care improvements for patients while ensuring CMS 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. The Committee should instruct the Administration to consider lessons learned and incorporate provider input on how to ensure the technology clinicians need and patients want is available. 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.

Our members are enormous proponents of technology, yet, they also understand the importance of the human touch. Technical innovation must flourish but it is also important to keep in mind the importance of fostering the connection between patients and their clinicians. We therefore believe 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.

Artificial Intelligence

We believe that technology has great potential to help achieve better care and greater efficiencies, such as artificial intelligence (AI). Yet it is critical to balance the drive for innovation and use of technology with the need to ensure that innovators understand the downstream ethical considerations that will determine the extent of adoption by the end-users – clinicians and patients. Such considerations may not be immediately apparent to innovators. However, they are significant for both clinicians and patients and will help determine the overall success of the innovation. We recognize that this balance is often a delicate one such that innovation is not stifled, yet ethical considerations must continuously be at the forefront as technology is being developed and rolled out.

Telehealth

Providers can inject innovation in care delivery when rules and reimbursement allow them to do so. Telehealth technologies offer a multitude of benefits to patients and clinicians. Increasingly our members are leveraging telehealth and remote monitoring services in a variety of ways to meet patient care needs. CHIME and KLAS Research conducted a detailed *study* in 2017 of 104 organizations currently administering telehealth programs. Some of the key findings include:

- 59 percent of respondents identified reimbursement as the biggest factor limiting expansion of telehealth services
- 34 percent of respondents noted cost or resources as a factor limiting expansion of telehealth services
- 59 percent of respondents cited improved patient access as a benefit of telehealth
- 35 percent of respondents cited improved clinical outcomes as a benefit of telehealth

All too often, telehealth is viewed solely as a benefit to small and rural hospitals that need to connect to clinicians at larger tertiary facilities. In fact, telehealth brings value to the entire delivery system. For instance, disease monitoring services can be a less expensive, more efficient and more convenient for patients with chronic conditions to stay connected with their care team. Telehealth services can also help minimize the risk of a readmission or bring video consultations to emergency departments. We are also seeing increased use of telepsychiatric screening. We also appreciate the additional authorities granted by Congress through the Balanced Budget Act of 2018 which permits Medicare to reimburse for more telehealth services.

The Committee should also consider how to address cross-state licensure concerns, often imposing troublesome legal barriers to a physician wishing to offer telehealth services to a patient in another state. Policies should allow licensed healthcare providers to offer services to patients, using telemedicine, regardless of what state a patient resides in, notwithstanding whether the patient is within a traditional care setting or in one's home. We applaud the Department of Veterans Affairs for taking on this issue for their patient population, and support the new rule that is now in place, "*Authority of Health Care Providers to Practice Telehealth*." We hope that we can learn from this VA initiative and address cross-state care provision concerns for the broader patient population.

Remote Patient Monitoring

Providers and health systems are encouraged by the potential of remote health monitoring but are still grappling with the realities of the wide-spread integration of these devices, such as wearables, into the provision of care. Our members acknowledge the value in collecting such

additional data, not only in real-time, but policies and procedures are still nascent. We would encourage the Committee to consider the value of wearables and remote monitoring technologies and ensure reimbursement paradigms are in place to support their expanded use. We applaud CMS for beginning to reimburse for this technology which will help spur greater uptake.

Bolstering Healthcare Cybersecurity

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.

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.

Policies are needed to help support providers secure their systems and patient data, and policies that reward good cybersecurity hygiene should be developed. Given the growth in federal policies towards increased data sharing, many of which are rooted in CMS, it is critical that cybersecurity remain at the forefront of policymaking rather than an afterthought. CHIME calls upon the Committee to address the growing nature of cybersecurity threats to patient data and ensure that security is included in any policy recommendations.

The evolving threat landscape and the persistent attacks from nation-state and professional entities seeking to cause harm to patients and health systems, demonstrate the need to revisit enforcement activity following an incident. Cybersecurity incidents have devastated even some of the nation's most well-resourced health systems. The Committee should encourage the Administration to evaluate their current enforcement discretion authority and penalty processes under HIPAA and HITECH to ensure existing policies are not unnecessarily "victimizing the victim".

The industry will benefit from the current efforts underway at CMS and the Office of the Inspector General (OIG) to examine new exceptions and safe harbors under the Stark and Anti-kickback statutes, including for cybersecurity services. Facilitating the donation of technologies and services to promote a stronger cyber posture among providers is welcomed. Congress should encourage CMS, however, to explore all possible avenues to supporting and incenting providers achieve this as cost continues to remain a barrier for many.

As the Committee monitors the implementation and administration of Medicare policies, we urge Members to ensure providers have access to technology necessary to facilitate their success in new payment models while ensuring CMS pursues reasonable policies that will reduce provider burden and facilitate greater care coordination.