College of Healthcare Information Management Executives

December 16, 2019

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

Re: Cures 2.0

Dear Congresswoman DeGette and Congressman Upton,

The College of Healthcare Information Management Executives (CHIME) is pleased to respond to your request for input for the development of Cures 2.0.

CHIME is a professional organization that represents more than 3,200 Chief Information Officers (CIOs) and other senior healthcare IT leaders. CHIME enables its members and business partners to collaborate, exchange ideas, develop professionally and advocate for the effective use of information management to improve the health and care in the communities they serve. CHIME members are responsible for the selection and implementation of clinical and business systems that are facilitating healthcare transformation through technology. Our members represent some of the earliest and most prolific adopters of electronic health records (EHRs) and other health IT resources. Our mission is, "To advance and serve healthcare leaders and the industry improving health and care globally through the utilization of knowledge and technology."

We appreciate the opportunity to share our thoughts on how we can build on the federal investments made in the health IT infrastructure in the Health Information Technology for Economic and Clinical Health Act (HITECH) Act and push for greater interoperability of health IT through 21st Century Cures Act to realize a data-driven healthcare ecosystem that should be the cornerstone of Cures 2.0. We applaud your commitment to bipartisanship and willingness to engage stakeholders as you pursue policy changes.

In addition to making recommendations for inclusion in future legislation, we will also outline some oversight opportunities for you and your colleagues to pursue as it relates to the implementation of the 21st Century Cures Act.

Implementation and Oversight of the 21st Century Cures Act

CHIME applauds your recognition of the need to spur nationwide health data interoperability in order to improve access to lifesaving treatments through the inclusion of numerous health IT provisions of the 21st Century Cures Act (Cures). Robust healthcare data exchange will be paramount as the industry seeks to move from volume-to-value through a focus on personalized medicine. It will be critical for the Administration, with Congressional oversight, to ensure that the policies generated out of the Cures Act spur data exchange that is reliant on solid data standards.

ONC Interoperability & Information Blocking Rule

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 support proposed provisions that were mandated by Cures to advance the nation's ability to leverage health information technology 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.

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 of patient data to third-parties and resultant harm. While it's important that Congress ensure that the Administration is furthering the objectives of Cures, the final regulations do not unreasonably increase provider burden or hinder patient care.

CHIME joined[1] six other provider organizations earlier this year in making recommendations that the regulations implementing Cures incorporate the following:

- **Additional rulemaking related to information blocking 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 Congress 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 enough time to deploy and test these systems, which must consider 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.

Additionally, the ONC proposed rule does not, in its current form, appear to include those technology companies that manage apps, nor does it cover the third-party apps themselves under proposed data blocking policies as among the actors who must comply with these policies. Therefore, unless these policies are changed, a big chunk of the healthcare sector like providers and EHR vendors will have to abide by one set of rules governing promoting the sharing of patient information, and third-party apps and those managing the app ecosystem will not. This will create an unlevel playing field and further perpetuate the notion that healthcare apps are the Wild West.

Data Privacy

Daily headlines indicate citizens have little idea how their healthcare data is being used by third parties where they either intentionally shared their data or where it was shared without their

[1] https://chimecentral.org/wp-content/uploads/2019/09/HIT-Provider-Group-Letter-to-Senate-EC-FINAL.pdf

knowledge. These incidents speak to the need for greater oversight. We are particularly concerned that as more citizens 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. Given the volume of data in question and the fact that this is sensitive healthcare data, this is cause for concern.

API Security
The CMS and ONC rules intended to improve patient access to their data and as directed by the 21st Century Cures Act, are aimed at achieving this goal. As you know, these rules call for advancing patient access to their data using APIs. Our members strongly support patient access to their medical data. However, they have significant privacy and security concerns associated with the transfer of this data to third parties. We are very worried that patients are unaware of how their data is being used once it is released and, in some cases, may be under the false impression that it is still safeguarded under HIPAA.

Given the speed with which CMS and ONC are moving to further facilitate patient access to their data via APIs, we worry that appropriate oversight must be in place to govern how patient data is not just accessed by third parties but also how it is being used. In short, patients must be able to trust the apps they are sending their data to and have full awareness when their data is being sold or used for marketing purposes. Although we raise these concerns in our response to ONC and CMS, and in subsequent joint communications with the Administration, we must stress the potential for complete loss of consumer and patient trust in apps if their data is mishandled. Further, once data is released, while data sharing can be revoked, there is no way to walk back what has already been shared. Moreover, the ability to monetize data is only growing.

Non-HIPAA Covered Entities
Our members take seriously their responsibility to safeguard and keep private patient information as required by HIPAA. Once a patient's medical record is downloaded via an open API to an app at the patient's request, that information is no longer protected by HIPAA unless the app is sponsored by a HIPAA-covered entity. Worrisome is that patients may not understand: 1) that HIPAA no longer applies; and 2) how the app intends to use their data. The terms and conditions may be lengthy, and patients may skip over them in favor of convenience. The terms and conditions also may or may not specify that the app developer could re-use or sell their data – including sensitive data – to others like third party data brokers. Our members are concerned that one bad actor could destroy consumer and patient trust in healthcare apps, dismantling efforts to further interoperability and improve patient access to their information. Our members believe more education is needed so that patients are fully aware of the benefits and risks associated with their data being reused without their knowledge.

In addition to what CMS and ONC have proposed, we acknowledge that the Office for Civil Rights (OCR) is considering changes to HIPAA as they contemplate the current data-rich environment, patients' needs for their data, and the need to foster better care coordination. Recently, the agency published a series of questions concerning a patient's right to access their information making it clear in one answer (Q/A) that, "The HIPAA Rules do not impose any restrictions on how an individual or the individual's designee, such as an app, may use the health information that has been disclosed pursuant to the individual's right of access."

As smart phones, social media and other apps become integral parts of everyday life, the definition of "healthcare data" is changing. Companies tracking location, payments, or both can easily discern if a patient is sick, how sick the patient is, or what type of illness the patient has. For example, a cancer patient drives to her specialist and has an hour-long appointment. She brings her phone, and in the waiting room, she may open her Facebook, Instagram and web search apps. All three apps collect location data, and all three apps can collectively know she is seeing a cancer specialist. That data is then aggregated and sold to third-party data brokers, making her extremely sensitive illness known to

faceless companies and people. A recent story in the New York Times outlined just how much data apps are collecting – some of it health – and demonstrated how easy it was to ascertain the whereabouts of citizens using location tracking data, including visits to a family planning clinic and a dermatologist's office[2]. The article also noted just how lucrative the location data is – estimated to be $21 billion in 2018.

While we have called on ONC to act quickly to bring needed clarity to the collection and use of healthcare data by third-party apps through their forthcoming interoperability rule, we also highlight the need for a robust national dialogue on healthcare privacy and call on Congress to request ONC address these issues in their final rule. As outlined above, the lines between health data and consumer data are blurred, and therefore, we need an approach to data privacy that spans the evolving nature of data exchange and use across the broader healthcare ecosystem.

Administrative Burden

On November 20, 2018, ONC, along with the 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. We commend you on inclusion of this strategy in the 21st Century Cures Act as too often technology not only serves as a burden to care providers, but it can impede patient care.

Technical innovation must flourish, as intended in the 21st Century Cures Act, but it is also important to keep in mind the importance of fostering the connection between patients and their clinicians. It's important that you encourage HHS to 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, formerly known as the Meaningful Use 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.

Policies are necessary to 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.

Too often our members have experienced policymaking that may be contradictory, duplicative or changed at the last minute. Competing regulatory priorities too often impede a health system's ability to invest in the technologies providers or patients want, instead needing to focus limited resources on the latest reporting module or system upgrade as to meet another mandate from Washington. We would encourage you to explore what direction may be needed within HHS to ensure that they can be more adept at sequencing regulatory compliance deadlines and investments in the technology needed to meet those deadlines. A clear roadmap is needed for providers with sufficient time to deploy new technology mandates.

We encourage you to pursue an evaluation of health IT programs to-date. A value analysis should be conducted on industry gains made, outcomes improvement but also costs. Costs should include a financial evaluation but also the implications for productivity, innovation and workforce strain. This

[2] 3 Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, New York Times, December 10, 2018

should include the HITECH programs, Medicare Access and CHIP Reauthorization Act (MACRA), Information Blocking, the Trusted Exchange Framework and Common Agreement (TEFCA), Appropriate Use, Electronic Prescribing of Controlled Substances (EPCS), the various federal quality reporting programs, just to name a few. Finally, special attention should be paid to the impact on rural and under-resourced providers, as well as, the impact on those clinicians and providers not eligible for HITECH incentives.

Patient Identification

Foundational to coordinated care is the need to accurately identify patients and match them with their healthcare data across providers, systems' public health agencies and states. A national approach to patient identification is prerequisite for health information exchange and the lack of a national standard for patient identification only serves to aggravate our industry's technical challenges.

The 21st Century Cures Act included the directive for a Government Accountability Office (GAO) report[3] on patient matching, which was released earlier this year. While a national approach to patient matching would be an important step toward true interoperability, without a standard patient identifier, the creation of a complete and accurate longitudinal care record is simply not feasible. A longitudinal healthcare record, supported by widely adopted standards, also should improve a patient's ability to manage consent privileges and diminish privacy concerns related to the digitization of personal health information.

We share your commitment to pursuing bipartisan solutions to solving critical health challenges, including the need to enhance outcomes, improve patient safety and combat the opioid epidemic by consistently identifying patients when they are seeking care. As was highlighted in the GAO report, today, there is no consistent approach to accurately match a patient to their health information, which has led to significant costs to hospitals, health systems, physician practices, long-term, post-acute care (LTPAC) facilities, and other providers. According to a 2016 study of healthcare executives, misidentification costs the average healthcare facility $17.4 million per year in denied claims and lost revenue. Another study indicates that patient misidentification costs the U.S. healthcare system over $6 billion annually.

Among the policy barriers that should be highlighted is the current prohibition on the use of federal funds to promulgate or adopt a patient identifier which has been carried forth in Labor-Health and Human Services Appropriations bills since fiscal year 1999. Without a standard patient identification solution, the creation of a longitudinal care record is simply not feasible. We encourage you to examine the issue of patient identification to facilitate nationwide interoperability, enhance patient safety and enhance health outcomes.

We urge you to build upon the GAO report released in January and consider legislative solutions to ensure patients are accurately identified and matched to their data. This could include a discussion of expansion of the Medicare Beneficiary Identifier (MBI) created through MACRA, beyond the Medicare population.

Digital Health

Hospitals, health systems and other providers are embracing the use of telehealth technologies because they offer benefits such as the ability to perform high-tech monitoring without requiring patients to leave their homes. This can be less expensive and more convenient for patients, as well as improve access to specialists and expand care to patients in remote locations. Telehealth services come in many forms, from post-discharge remote patient monitoring (RPM) programs resulting in reduced hospital readmissions, to emergency departments using remote video consultations to enable patients to receive a telepsychiatric screening. Yet, whether public and private payers cover telehealth

[3] Gao.gov. (2019). *Health Information Technology: Approaches and Challenges to Electronically Matching Patients' Records across Providers*. [online] Available at: https://www.gao.gov/products/GAO-19-197.

services and adequately reimburse hospitals and other healthcare providers for providing those services, is a complex and evolving issue. As a result, reimbursement is often a barrier to standardizing the provision of these valuable services. Most of our members cannot afford to invest in telehealth technologies in the absence of robust reimbursement by payers.

Further, CHIME members would like to highlight that although the technology may be available, and interest exists among providers and patients to leverage telehealth and RPM technologies, the communications requirements to effectively use such technologies may render the programs useless.

Access to broadband
Our members highlight that one significant barrier hindering adoption of telehealth and RPM by patients and providers alike is broadband access.

A recent Agency for Health Research & Quality (AHRQ) report[4] states, "Rural primary care facilities may also experience challenges implementing health IT or telehealth solutions due to a lack of broadband access. Broadband availability is incredibly important for both providers and patients to use these innovative systems and platforms. According to the Federal Communications Commission's (FCC's) 2016 Broadband Progress Report, 23 million rural Americans lack access to broadband at benchmark speeds. Moreover, individuals and practices in rural areas who do have access to broadband may end up paying three times more for these services than their urban counterparts." We agree that all of these areas represent barriers. We also see persisting barriers in rural areas and these areas must not be forgotten either. By some accounts approximately a quarter of those living in cities still don't have broadband access either."

CHIME supports Congressional efforts to address broadband access disparities across the nation and suggest you consider ways to expand access where broadband may not be possible. In fact, we recommended the FTC double the funding available under their Rural Health Care (RHC) Program from $400 million annually to $800 million. Ultimately the agency opted for a 40% increase to $571 million, the first such increase since the program was created in 1992. This increase will allow greater reach of telehealth in rural and remote areas, yet more help is needed to keep pace with demand.

5G
In considering the best way to reach rural and hard-to-serve communities (which include urban areas), we highlight the promise of 5G. The ultra-low latency and high-speed capability of the 5G networks may not only remove existing access barriers but also unlock the ability for the world's best doctors and specialist to diagnose and treat patients in these areas. Simply, 5G may connect patients with healthcare providers in ways not possible today and redefine every aspect of healthcare. The possibilities include video visits, patient monitoring, remote diagnostics, prescription adherence, connected internet of things (IoT) sensors and more. Thus, CHIME encourages you to pursue policies to enable the proliferation of 5G; this should start with a GAO report on the applications of and opportunities for a 5G in healthcare.

Data Usage Limitations
While broadband access may be a challenge in rural areas, where our members are leveraging RPM technologies that are internet-enabled, patients on limited data plans may be prohibited from taking advantage of the services. One children's hospital CIO offered the example of a child outfitted with a Cochlear implant, a surgically placed electronic device, which can be transformative for a child's development and future. But it's not a one-and-done event. Because recipients haven't always been able to have the same speech-teaching interactions that hearing children do, life with a new Cochlear implant can involve significant, specialized speech therapy requiring weekly visits. One of the key questions when evaluating a child as a Cochlear implant candidate is whether he or she will be able

[4] "Implementing Medication-Assisted Treatment for Opioid Use Disorder in Rural Primary Care: Environmental Scan Volume 1." Available at: https://integrationacademy.ahrq.gov/sites/default/files/mat_for_oud_environmental_scan_volume_1_1.pdf

to attend these visits. The innovative use of telespeech to bring speech therapy into patients' homes breaks down barriers to care for patients in remote areas who previously would have been denied access to Cochlear implants, or whose families would have had to make enormous sacrifices to travel for their therapies. However, if these families lack access to the internet for these telehealth visits, which may need to be conducted via smart phone using a data plan, they too would be precluded from receiving the implant.

Addressing Reimbursement Challenges

We commend you for including the request for a study of telehealth in Medicare in the 21st Century Cures Act. As was mentioned in the study, telehealth use in Medicare Fee for Services (FFS) remains very limited and this echoes what we continue to hear from the CHIME membership. In 2017 CHIME partnered with KLAS Research on a study titled "Telehealth Virtual Care Platforms 2017: An Early Look at the State of Telehealth." The study found, "The greatest limiting factor to the successful growth and expansion of telehealth is reimbursement—more than half of study respondents have concerns about this. Insurance companies, Medicare/Medicaid, and ACOs have been slow to reimburse telehealth visits, with Medicare lagging the most. When providers are reimbursed, it is often for less than the costs incurred; this disincentivizes providers since they can be paid more for in-person visits, and it makes it hard for some health networks to make a business case for telehealth solutions."[5]

The study found healthcare organizations used their virtual care platform vendor in one or more of three primary visit types:

- *Scheduled/patient focused – to increase patient access by allowing patients to schedule and conduct a clinical visit virtually*
- *On-demand/consumer focused, to decrease the costs for patients and providers by dealing with urgent/nonemergency medical needs of patients on-demand consultations – to improve the clinical outcomes of patients by increasing their access to needed specialists.*

The study raised questions about cost, reimbursement, available technology, value, the patient experience and integration. The majority surveyed said they plan to either expand the number of specialties served or expand patient access to providers using telehealth systems. They listed patient convenience among the top benefits. This is promising for telehealth; whose success ultimately hinges on patients' embrace of this healthcare delivery vehicle. Three-quarters of respondents reported that they were actively planning to either expand the number of specialties served or expand patient access to providers using their present solution.
Some key findings include:

- 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
- 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
- 70 percent of respondents said their telehealth platforms have no integration with their electronic health record (EHR)

Although Medicare has slowly incorporated additional telehealth services into their reimbursement models, including telestroke and teledialysis as included in the Balanced Budget Act of 2018, there are still significant geographic and definitional limitations. Geographical limitations currently restrict coverage of telehealth services. The demand for "parity" in reimbursement for services provided in-person by a physician and those via telemedicine has never been greater. The realignment of federal payment structures is a key factor to increasing access to telehealth services and warrants further Congressional action.

[5] Telehealth Virtual Care Platforms 2017 An Early Look at the State of Telehealth, available at: https://chimecentral.org/wp-content/uploads/2017/09/Telehealth-Virtual-Care-Platforms-2017-CHIME-Industry-Version-FINAL1.pdf

Inconsistencies in the definition and reimbursement policies of telehealth services in federal and state programs are hurdles to widespread adoption. While Medicaid encourages states to use flexibility to create innovative payment methodologies for services that incorporate telemedicine, there are still significant coverage gaps from state to state. Differences in state laws, definitions and regulations create a confusing environment for hospitals and health systems that may care for a patient across state lines.

Further, we encourage you to 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. CHIME supports policies to 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 his or her home.

Remote Monitoring

KLAS Research conducted a study titled, "Remote Patient Monitoring 2018 High Potential in a Shifting Landscape"[6] that found that many provider organizations start with one or two specific patient conditions and then expand their monitoring to others over time as they became more comfortable and confident in their vendor's solutions and in their own capabilities. Among the 25 organizations that participated in the study, heart disease and chronic obstructive pulmonary disease (COPD) were the most common conditions treated under programs, followed in frequency by diabetes and hypertension. It will be critical that federal reimbursement programs enable clinicians and patients to take advantage of RPM technologies as a broader examination of digital health policy ensues.

Interoperability Across the Care Continuum

We would also emphasize the impact of discrepancies in technology adoption across the care continuum. While the Meaningful Use program incented the adoption of EHR technology by most providers, hospitals and critical access hospitals (CAHs), other care settings were not included. Today post-acute and long-term care facilities and behavioral health providers often do not have the resources to implement and use EHR technology. For this reason, CHIME supported the provision included in the SUPPORT Act that promotes testing of incentive payments for behavioral health providers for adoption and use of certified electronic health record technology. This model should be considered for the long-term post-acute care community as well. To have true interoperability, records should be complete and include all care encounters, not just those in clinician offices or hospitals.

Modernizing 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 type, and similar to most privacy policy, there is no national consent policy. Consent challenges have been highlighted in efforts to thwart the opioid epidemic through data sharing, specifically the impediment to sharing substance use disorder (SUD) data imposed by the lack of alignment with HIPAA and 42 CFR Part 2. 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, including SUD data. This should include re-examining certain provisions of HIPAA. While the Office for Civil Rights (OCR) has begun a review, Congressional action will be needed. CHIME supports the Protecting Jessica Grubb's Legacy Act (S.1012/ H.R. 2062) and we encourage you to consider it for inclusion in this important package.

[6] Remote Patient Monitoring 2018 High Potential in a Shifting Landscape, available at: https://klasresearch.com/report/remote-patient-monitoring-2018/1273

Device Cybersecurity

Healthcare has entered an era of ubiquitous connection, and the internet of things (IoT) is transforming healthcare along with the world's economy. Tens of thousands of medical devices can be used throughout large healthcare systems, many of which are connected directly to the patient or serving to provide information to inform clinical decision making. Wearables and medical devices are being directly connected to EHR systems, which generates additional data for clinical decision making but also increases the threat surface.

To "Transform Medical Device Safety, Cybersecurity, Review, and Innovation" FDA requested $55 million, which includes the creation a cybersecurity unit to complement the advances in software-based devices as well as to aid in review of cybersecurity advances affecting the more traditional, hardware- and software-based medical devices. The FDA budget justification states:

> *"Currently, there is no statutory requirement (pre- or post-market) that expressly compels medical device manufacturers to address cybersecurity. This proposal would advance medical device safety by ensuring FDA and the public have information about the cybersecurity of devices. Specifically, FDA seeks to require: that devices have the capability to be updated and patched in a timely manner; that premarket submissions to FDA include evidence demonstrating the capability from a design and architecture perspective for device updating and patching; a phased-in approach to a Cybersecurity Bill of Materials (CBOM), a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities; and that device firms publicly disclose when they learn of a cybersecurity vulnerability so users know when a device they use may be vulnerable and to provide direction to customers to reduce their risk. The proposal also seeks to improve proactive responses to cybersecurity vulnerabilities."*[7]

Cybersecurity incidences like Petya and WannaCry demonstrated how vulnerable some network connected devices can be, thus we support the FDA's efforts to secure the healthcare sector. As the FDA states, "Newer devices are more often interconnected and interoperable, increasing cybersecurity threats." Viewing security as a component of safety and efficacy of device functions and embracing "security by design" are necessary to keep pace with these variable threats. A secure healthcare system will ultimately enable greater consumer confidence and will spur better care coordination, enhanced information exchange and improved patient care.

We applaud the Device Program's goal to encourage a coordinated approach of vigilance, responsiveness, resilience, and recovery with respect to cybersecurity that fits the culture of continuous quality improvement. The FDA states that this equates to taking a total product lifecycle approach, starting at the product design phase when FDA builds in security to help foil potential risks, followed by having a plan in place for managing any risks that might emerge, and planning for how to reduce the likelihood of future risks. Specifically, FDA states that medical device manufacturers are encouraged to proactively update and patch devices in a safe and timely manner. The concept of updates and patches, while not new to traditional information technologies, is complex when it comes to critical safety systems and requires a collaborative approach to finding solutions. FDA has published guidance documents – recommendations for manufacturers and others – that contain recommendations for comprehensive management of medical device cybersecurity risks throughout the total product life cycle. This includes closely monitoring devices already on the market for cybersecurity issues. To enable more expedient actions, the Device Program's overall approach incentivizes industry to make changes to marketed and distributed medical devices to reduce risk.

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. This vulnerability increases as medical devices are increasingly connected to the Internet, hospital networks, and other medical devices, and as

[7] Department of Health and Human Services Fiscal Year 2020 Food and Drug Administration Justification of Estimates for Appropriations Committees, Available at: https://www.fda.gov/downloads/AboutFDA/ReportsManualsForms/Reports/BudgetReports/UCM633738.pdf

patients demand greater access to their information in more nimble ways like via APIs on third-party mobile apps. In recent years, FDA, manufacturers, and healthcare entities have made tremendous strides to improve the cybersecurity of medical devices. We would encourage you to work with the FDA to ensure they have the authority necessary to ensure the safety and security of medical devices.

Transparency for Clinical Decision Support
We appreciate your intent in the Cures Act to address the regulatory schematic for clinical decision support (CDS) technology, but much confusion has ensued since enactment. We believe that it is important for the FDA to have the authority to regulate CDS and black box algorithms alike, leaving the FDA to decide to exercise enforcement authority based on an appropriate risk profile. Further, there must be transparency, so clinicians understand in making clinical judgements using CDS and when machine learning (ML) is relied upon that there is an understanding around how this technology works and the basis for how decisions reached.

CHIME commends your willingness to engage stakeholders to pursue policies to build on prior bipartisan efforts to improve healthcare and spur access to life-saving treatments. We hope our comments 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 Mari Savickis, Vice President of Public Policy, at mari.savickis@chimecentral.org .

Sincerely,

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