June 26, 2020

The Honorable Lamar Alexander
Chairman
Senate Committee on Health, Education,
Labor & Pensions
U.S. Senate
Washington, D.C. 20510

Dear Chairman Alexander,

The College of Healthcare Information Management Executives (CHIME) is pleased to have the opportunity to submit comments in response to your white paper, Preparing for the Next Pandemic, and commends you for your leadership on this issue.

CHIME is an executive organization dedicated to serving more than 3,200 chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. 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. Our mission is, "To advance and serve healthcare leaders and the industry improving health and care globally through the utilization of knowledge and technology."

CHIME recommends that the Senate Committee on Health, Education, Labor & Pensions ("The Committee") prioritize the following items in future pandemic preparedness legislation so that our nation is better prepared for the next pandemic:

I. Protect Telehealth

Extending Current Telehealth Flexibilities

CHIME agrees with Recommendation 4.2 and believes the telehealth gains made in the United States since the start of the pandemic must be supported if the health system wants to continue to safely treat patients, preserve personal protective equipment (PPE) and maintain a healthy clinician workforce. The U.S. has hit another daily case record, some states are delaying re-openings, and new Centers for Disease Control & Prevention (CDC) data points to several states seeing an uptick in cases.

Since the outbreak of COVID-19 began, we have heard from our members about the struggles and successes those on the front lines have experienced in fighting the pandemic. A common refrain from those members is that telehealth and the ability for patients to access care at a

distance is critical to fighting this disease. While those in current hotspots are working to flatten the curve by treating patients in critical need of emergency services in person, they also highlighted the need for patients who are infected, but stable, to be able to access care without infecting other providers or fellow patients. Those who are not yet part of the growing infected population should remain home to protect both healthcare workers and other patients they may come into contact with during a visit. Conversely, other members in communities yet to be heavily impacted by COVID-19 are also working to prevent their infection rate from ever reaching a level that would strain their system and services by utilizing telehealth. These providers continue to embrace the available flexibilities to ensure they can limit any unneeded or dangerous interactions patients and providers may have. Furthermore, patients continue to demand access to telehealth services, even more so now with wider availability of telehealth.

CHIME Recommendation #1: To ensure that the United States does not lose gains in telehealth, the current telehealth flexibilities must stay in place for at least 24 months. We detail the basis for this recommendation in a letter to Congressional leadership we sent on June 16.

Abruptly withdrawing these policies will undermine efforts to fight the spread of the disease. Additionally, it will put unneeded strain on our already stretched medical professionals and pose unnecessary threats to patient safety. Importantly, this will also allow enough time for Congress and CMS to collect and analyze data that can be used to determine which flexibilities should be extended or made permanent. Today there are several agencies (i.e. Veterans Affairs, Federal Communications Commission (FCC)) involved with the payment and support of telemedicine and taking a coordinated and holistic approach to evaluating it will be important.

If only pieces of the flexibilities can be extended for the 24-month period, we request that Congress consider extending flexibilities granting:

- A moratorium on the rural or distanced site requirements for both patients and providers
- Removal of the established patient requirements for telehealth
- Reimbursement parity for audio-only telehealth services
- Reimbursement parity between in-person and telehealth provided services
- Reimbursement parity for rural health clinics (RHCs) and Federally Qualified Health Centers (FQHCs)
- Waiver of cross-state licensure requirements for providing telehealth

CHIME Recommendation #2: Establish an Office of Telehealth within the Office of the Secretary of the U.S. Department of Health & Human Services (HHS) to prioritize the ongoing evaluation, measurement and coordination with other federal partners on telehealth activities to support this care modality.

Expanding Access to Broadband and 5G

Virtual health technologies, coupled with current federal policies under the pandemic allow providers to meet patients where they are, in their home, and permits for the use of remote patient monitoring to allow those providers to continually treat their patients after the initial visit. These and many other technologies exist to transform how healthcare is delivered and pushes the way care is delivered into the 21st century. Virtual health can improve outcomes and currently helps the healthcare sector contain the spread of COVID-19. All of these improvements in virtual health technology is predicated on the ability of providers and patients to have access to reliable high-quality broadband services – such as dedicated 5G – as many technologies require the use of both complex audio and video technologies. The COVID-19 pandemic has yet again highlighted challenges faced by many providers and patients where broadband access is limited, creating more disparities in care.

The global pandemic has further solidified technology's place in healthcare, as well as the world in general, and the need for dedicated high-speed internet service has never been greater. As more activities are available and more devices are connected via the Internet, bandwidth and latency become increasingly relevant, particularly for the provision of high-quality healthcare. To ensure consistent access to new healthcare tools, it is essential that plans for addressing the digital divide include provisions to provide access to 5G networks throughout this country, regardless of population density or terrain.

The migration to the fifth generation of high-speed wireless networks, or 5G, will allow technologies to truly revolutionize healthcare. Removing today's bandwidth limitations brings endless possibilities for the proliferation of telehealth and remote monitoring; the unleashing of augmented or artificial intelligence (AI) and big data; and, the optimization of healthcare operations. Untethering patients from the capabilities of a traditional network will alter patient engagement and mitigate existing access challenges. Faster speeds combined with cloud-based storage will enable advanced digital networks capable of generating and leveraging large quantities of data in ways previously unimaginable. As has been made evident during the current crisis, care can be delivered virtually anywhere at any time to anyone. There's no question that the infusion of 5G into healthcare will enhance access to care, while decreasing costs and improving efficiency.

CHIME Recommendation #3: **Increase funding for the Rural Health Care (RHC) program at the FCC to support providers' ability to upgrade their broadband connectivity and expand their telemedicine services.**

II. Modernize the Digital Health Infrastructure

Supporting Removal of the UPI Appropriations Ban

The COVID-19 pandemic has highlighted even more examples of why the removal of the federal unique patient identifier (UPI) appropriations ban in place since 1999 is holding back our ability to deliver safe and effective care. Aggregating surveillance, as discussed in the white paper, requires accurate and timely information to identify where diseases are spreading. Aggregated data is only as good as what is collected. One important way this can be improved is by ensuring patients can be correctly identified and matched with their records.

As stated in a recent paper by the Office of the National Coordinator for Health Information Technology (ONC), "High-quality patient demographic data is fundamental to accurate patient identification and matching. Consequently, accurate patient identification and matching is pivotal to interoperability, quality of care, patient safety, and research" (Patient Matching, Aggregation, and Linking (PMAL) Project, ONC, August 2019). Also, as described in a FAQ on the website of the CDC's National Health Safety Network:

> ***Q15: Which Patient ID should be used when reporting data to NHSN: the visit/account number or the medical record number?***
>
> *The patient ID is the key identifier in NHSN for each facility. Therefore, the patient ID should be an identifier that remains constant for the patient on any subsequent visits; oftentimes, this is the medical record number. The use of an identifier that changes with each visit to the facility, for example, would result in the inability to link an SSI to a procedure, as well as inappropriate assignment and calculation of LabID events and subsequent measures.*

Unfortunately, until the appropriations ban (Section 510) which prohibits HHS from using funds to "promulgate or adopt any final standard …. providing for the assignment of a unique health identifier for an individual" is removed, our ability to accurately identify and match patients to

their records is stymied. Not only is this a threat to patient safety, it creates unneeded costs to the healthcare system, including federal entities like the CDC and National Institutes of Health (NIH), who are large aggregators of patient data. Our members use extensive resources to untangle duplicate records and match patients to their records. This is an expense that the nation cannot afford from an interoperability, patient safety and cost standpoint.

CHIME Recommendation #4: Congress should omit the 1999 language in FY21 Appropriations Legislation:

> ***SEC. 510. None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard.***

Reviewing Health IT Mandates

In May ONC and CMS released landmark regulations following through on mandates contained in the 21st Century Cures Act ("Cures"). These new information blocking and interoperability requirements are intended to usher in greater ability to exchange information across the care continuum. We recognize that this will require hard work by both providers and vendors. In looking ahead to what will be required, our members still must meet dated, legacy health IT requirements stemming from the Health Information Technology for Economic and Clinical Health Act (HITECH), a law enacted more than a decade ago. While Promoting Interoperability (formerly Meaningful Use) requirements have been updated several times, we believe it is worth taking a fresh look at whether many of these requirements still hold merit. For instance, e-prescribing is widely deployed among hospitals and clinicians, yet it is still a requirement. Moreover, there are a myriad of other health IT-related mandates that fall outside of HITECH and Cures which are critical and will require significant effort by providers, such as the e-prescribing of controlled substances (EPCS) mandate starting January 1, 2021.

CHIME Recommendation #5: We recommend the Committee conduct outreach to provider stakeholders like CHIME to ascertain the value of older, legacy requirements as they focus on newer more relevant mandates to help best position providers for care delivery in the 21st Century.

Invest in Public Health Infrastructure

Public health agencies at the federal, state, local, tribal and territorial levels are actively working with healthcare providers and the public at-large to detect, report, respond to and prevent illness and death. Unfortunately, the nation's public health data systems are antiquated, rely on obsolete information sharing methods and are in dire need of security upgrades. There are five critical pieces to the surveillance system which require support: The National Notifiable Disease Surveillance System (NNDSS); Electronic case reporting (eCR); Syndromic surveillance; Electronic Vital Records System; and Laboratory Information Systems.

CHIME applauds Congress for providing $500 million for the CDC's Data Modernization Initiative to invest in better COVID-19 tools and build state and local public health data infrastructure.

CHIME Recommendation #6: We recommend Congress make a significant investment in the CDC's data infrastructure over the next decade to support 21st century data collection, surveillance and public health.

III. Strengthen Cybersecurity Infrastructure

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 we increase interoperability, additional threats to data integrity and patient safety will arise. Without proper safeguards, the safe and secure transmission of sensitive data will continue to be a challenge and will hinder efforts to improve outcomes.

The healthcare sector, despite making progress over the past several years, is ill-equipped to handle a concurrent pandemic and cyberattack. Unfortunately, that is what our nation's healthcare system could very well experience. Cyber criminals are fully aware of our vulnerabilities and experts are predicting they will capitalize on those vulnerabilities. Given the complexity of the ever-growing number of interconnected devices, it is important to guarantee the security of those devices and the networks they reside on. As 5G utilization grows, the industry must monitor its adoption for additional risks that may arise as the Internet of Medical Things (IoMT) continues to rapidly expand.

The added stress to our nation's healthcare providers as they treat those with or suspected to have COVID-19 brings heightened importance to fortifying their ability to maintain continuity of operations. One industry estimate found that since January there has been a **"**30,000% increase in phishing, malicious websites, and malware targeting remote users—all related to COVID-19" (Zscaler, April 2020).

Providers need additional support to fend off the growing and sophisticated attacks aimed at stealing intellectual property, extorting ransoms, threatening patients by targeting medical devices connected to patients and hindering their ability to deliver care overall.

CHIME Recommendation #7: We encourage the Committee to ensure that "modernization of infrastructure" includes initiatives to improve the digital and cybersecurity infrastructures of healthcare providers in addition to their physical infrastructure improvement needs. This includes funding for providers, as well as HHS' Health Sector Cybersecurity Coordination Center (HC3), a national asset that providers can turn to for advice and threat intelligence.

We thank you for your efforts in preparing our nation for the next pandemic and appreciate the opportunity to share our recommendations with the Committee. Should you have any questions about our positions or if more information is needed, please contact Cassie Leonard, Director of Congressional Affairs, at cleonard@chimecentral.org.

Sincerely,

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

John Kravitz
Chair, CHIME Board of Trustees
CIO, Geisinger