2017 BOARD OF TRUSTEES
Liz Johnson, MS, FAAN, FCHIME, FHIMSS, CHCIO, RN-BC
(Chair) *Tenet Healthcare*

Marc Probst, CHCIO (Foundation Chair)
Intermountain Healthcare

Russell Branzell, FCHIME, CHCIO
(President & CEO) - CHIME

Zane Burke (Foundation Rep.)
Cerner

Marc Chasin, MD, CHCIO
St. Luke's Health System

Myra Davis
Texas Children's Hospital

Kali Durgampudi (Foundation Rep.)
Nuance Communications

Cletis Earle
Kaleida Health

Steve Eckert (Foundation Rep.)
Divurgent

Carina Edwards (Foundation Rep.)
Imprivata

David Finn (Foundation Rep.)
CynergisTek

Dennis Gallitano, Esq. (General Counsel)
Gallitano & O'Connor LLP

Michael Martz, CHCIO
Ascension Information Services

Theresa Meadows, RN, CHCIO FHIMSS, FACHE
Cook Children's Healthcare System

Frank Nydam (Foundation Rep.)
VMware

Albert Oriol
Rady Children's Hospital-San Diego

Shafiq Rab, MD, CHCIO
Rush University Medical Center

Donna Roach, CHCIO, FHIMSS
Via Christi Ascension Information Systems

Jan-Eric Slot (International Rep.)
Bernhoven Hospital

October 27, 2017

The Honorable Eric D. Hargan
Acting Secretary, U.S. Department of Health & Human Services
200 Independence Avenue, SW
Washington, D.C., 20201

Dear Acting Secretary Hargan:

Every four years the U.S. Department of Health & Human Services (HHS) updates its strategic plan. The College of Healthcare Information Management Executives (CHIME) is pleased to offer our comments on the HHS draft Strategic Plan, FY 2018-2022. CHIME is an executive organization serving more than 2,400 chief information officers (CIOs) and other senior health information technology leaders at hospitals and clinics across the nation. CHIME members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation.

HHS has articulated the following five strategic goals under the draft plan:

1. Reform, Strengthen, and Modernize the Nation's Health Care System
2. Protect the Health of Americans Where They Live, Learn, Work
3. Strengthen the Economic and Social Well-Being of Americans across the Lifespan
4. Foster Sound, Sustained Advances in the Sciences
5. Promote Effective and Efficient Management and Stewardship

While each of these goals is laudable, our comments will be limited to two areas. The first area is cybersecurity and the second is the ability of healthcare systems to interoperate. From our vantage point, we believe these topics are so impactful that they span almost all of the entire healthcare system and have implications for the success of HHS' five goals. Like so many other industries, healthcare has experienced a digital revolution that is changing the way care is delivered, cures are developed, diseases are diagnosed, outcomes of care are impacted,

College of Healthcare Information Management Executives (CHIME)
710 Avis Drive, Suite 200 | Ann Arbor, MI 48108 | 734.665.0000 | www.chimecentral.org

information is shared, and patients are engaged – to name a few. Although the strategic plan addresses several important objectives, it does not adequately highlight in many areas the role technology plays in changing the face of our healthcare system.

First, we worry an insufficient amount of attention is being paid to the risks of cyber threats. Our healthcare system is under attack by sophisticated nation states and criminal enterprises intent on stealing patient information and intellectual property, exacting ransoms while holding healthcare providers and other healthcare entities hostage, and penetrating important layers of our healthcare system. Healthcare is one of sixteen critical infrastructures that lags several other critical infrastructures in its capability to respond to cyber attacks. Congress recognized this when they passed the Cybersecurity Information Sharing Act (CISA) in 2015 as part of the Consolidated Appropriations Act of 2016. This law directed HHS to form a Health Care Industry Cybersecurity Task Force to offer recommendations on how to fortify our sector. The Task Force delivered more than 100 recommendations earlier this year that paint a dire picture of the state of readiness.

More importantly, the safety of patients is being placed at risk. A spate of articles published recently in prominent medical journals have showcased these concerns:

- An article published in the *Journal of the American Medical Association (JAMA)* earlier this month (October 10, 2017) focused on this very topic. The article's authors wrote that the move from a paper-based system to an electronic one, "has introduced unintended and unfavorable consequences, such as theft of patient-protected health information, wide-scale sequestering of medical records by ransomware (malicious software—malware—that permanently blocks the access to records unless a ransom is paid), and the ability for hackers to directly harm patients."
- An article in the *New England Journal of Medicine* (August 24, 2017) pointed to the repercussions stemming from compromised systems which pose threats that go beyond exposed protected health information. The author noted, "Manipulation of patient data could be even more damaging. An attacker with access to a laboratory system could modify data — changing potassium values, for example. Unsuspecting health care providers could react to the falsified potassium values, providing treatment that could harm the patient. Radiology protocols, diagnostic reports, genetic data, progress notes, and electronic prescriptions — the list of possible targets goes on. Protecting our information systems and our health data is critical to ensuring the safe delivery of health care." Authors of another article (June 7, 2017) published in the *New England Journal of Medicine* (NEJM) aptly titled, "Cyberattack on Britain's National Health Service — A Wake-up Call for Modern Medicine," found that the WannaCry cyberattack, "exposed the fact that although much has been written about cyberattacks potentially breaching confidential patient information, health care providers have not truly considered the physical harm that could befall our patients should an external party with malicious intent take over health service computers."

While the Administration is pushing to elevate the posture of the Cyber Command to be its own unified military command, the healthcare sector as a whole lags behind other critical infrastructures and is increasingly vulnerable to the earlier referenced attackers. We believe that the role cybersecurity defenses play in healthcare is an infrastructure issue that must be addressed for the good of all Americans. We, therefore, appreciate that HHS has acknowledged cybersecurity under objectives 5.4: "Protect the safety and integrity of our human, physical, and digital assets." That said, we believe more attention is warranted. We also are pleased to see HHS' attention to workforce; there are 65 mentions of the word workforce in the document. We did not see, however, a focus on the need to cultivate a cyber workforce to keep pace with the growing demands and threats in this space. Having an adequately trained workforce will be critical to achieving the priorities we have outlined. **We call on the Department to prioritize cybersecurity both within the Department and across the sector. The recent attacks and referenced articles should serve as a call to action for the industry to collectively pursue actions to improve our cybersecurity posture including devoted increased attention to building and sustaining an amply equipped workforce to tackle increasing cyber threats.**

Second, it is our belief that an interconnected and interoperable healthcare system will improve patient care, expand access to care, facilitate better outcomes, improve diagnosis and treatment, reduce costs and facilitate scientific breakthroughs. We appreciate that HHS has discussed its plans for facilitating "information sharing, exchange and alignment" under objective 4.1 and standardizing public health data collection, aligning incentives and promoting evidence-based guidelines. But we believe a stronger focus will be needed to achieve work that

College of Healthcare Information Management Executives (CHIME)
710 Avis Drive, Suite 200 | Ann Arbor, MI 48108 | 734.665.0000 | www.chimecentral.org

began in earnest at HHS in 2004 to facilitate a more interoperable healthcare system and which remains a sought-after goal in our system to this day. **The 21st Century Cures Act calls on HHS to establish a new, highly anticipated Health IT Advisory Committee to focus on helping HHS advance interoperability in the healthcare sector. This landmark piece of legislation and the provisions outlined around interoperability will be pivotal to advancing the Department's goals. We thus recommend a stronger focus in the strategic plan around fostering a healthcare system that is truly interoperable.**

Finally, we feel it important to highlight a persisting challenge that unless remedied, will continue to stymie a truly interoperable healthcare system – not to mention jeopardize patient safety – and that is the ability to successfully match a patient to their record. We understand that HHS is precluded from using their funds "to promulgate or adopt" a standard for the assignment of a unique patient identifier, according to language contained in the Labor-HHS Appropriations bill which has been included since 1999. There is however, language in the FY 2017 Appropriations House Labor-HHS report, indicative of a growing willingness to support private sector-led solutions. Specifically, the language states:

> *The Committee is aware that one of the most significant challenges inhibiting the safe and secure electronic exchange of health information is the lack of a consistent patient data matching strategy. With the passage of the HITECH Act, a clear mandate was placed on the Nation's healthcare community to adopt electronic health records and health exchange capability. Although the Committee continues to carry a prohibition against HHS using funds to promulgate or adopt any final standard providing for the assignment of a unique health identifier for an individual until such activity is authorized, the Committee notes that this limitation does not prohibit HHS from examining the issues around patient matching. Accordingly, the Committee encourages the Secretary, acting through the Office of the National Coordinator for Health Information Technology and the National Coordinator for Health Information Technology and CMS, to provide technical assistance to private-sector led initiatives to develop a coordinated national strategy that will promote patient safety by accurately identifying patients to their health information.*

Furthermore, we would also note that Section 4007 of the Twenty First Century Cures Act contains language that instructs the Government Accountability Office (GAO) to conduct a study on patient matching. In fact, a letter was recently signed by more than 25 organizations, including CHIME, calling for a collaboration between HHS and the private sector on patient matching and identification efforts. We urge HHS to continue working collaboratively with the private sector to overcome this pivotal piece to addressing widespread interoperability among disparate healthcare providers and other stakeholders.

In conclusion, our members are devoted to improving the American healthcare system through the use of technology. Based upon the feedback offered above, we recommend that HHS strengthen the language and objectives in the report to better focus on fortifying the nation's (both internal to HHS operations and external to the private sector) ability to keep pace with growing cyber threats and to focus on achieving a truly interoperable healthcare system. Doing so will benefit all of the goals outlined by HHS in the strategic plan.

Sincerely,

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

Liz Johnson, MS, FAAN, FCHIME, FHIMSS,
CHCIO, RN-BC CHIME Board
Chair; CIO, Acute Care Hospitals & Applied Clinical Informatics, Tenet Healthcare

College of Healthcare Information Management Executives (CHIME)
710 Avis Drive, Suite 200 | Ann Arbor, MI 48108 | 734.665.0000 | www.chimecentral.org