February 06, 2015

Karen B. DeSalvo, M.D., M.P.H., M.Sc.
National Coordinator for Health Information Technology,
Assistant Secretary for Health
Department of Health and Human Services

Re: Federal Health IT Strategic Plan 2015-2020

Dear Dr. DeSalvo:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to provide input to the Federal Health IT Strategic Plan 2015-2020 ("the Plan") orchestrated by the Office of the National Coordinator for Health Information Technology (ONC).

CHIME is a professional association representing more than 1,400 chief information officers (CIOs) and other top information technology executives at hospitals and clinics across the nation. CHIME members have frontline experience in implementing the kinds of clinical and business IT systems needed to realize healthcare transformation. Healthcare CIOs share the vision of an e-enabled healthcare system as described by the many efforts underway at the Department of Health and Human Services (HHS).

The effort needed to compile a unified strategy, spanning 37 federal departments and agencies, cannot be understated. CHIME applauds ONC for undertaking this important task. The Plan, as we understand it, represents a significant evolution in thinking among federal policymakers. Compared to the 2008 and 2011 Plans, we see vast improvements in how ONC is framing and detailing each goal, outcome and associated strategies. Delineating implementation responsibilities among federal agencies, for example, is an essential improvement and one we support.

CHIME continues to believe that we have a unique opportunity, over the next several months, to evaluate standing policies, address known policy shortfalls and make progress towards the future-state vision, articulated by this federal strategic plan. CHIME agrees overwhelmingly in the five goals espoused by the Plan and we see many of our own priorities engrained in the objectives listed, including strategies that:

- Advance technical and electronic methods to accurately identify, proof, match and authenticate information across data sources;
- Support, promote, and enhance the establishment of a single health and public health Information Sharing and Analysis Center (ISAC) for bi-directional information sharing about cyber threats and vulnerabilities between the private health care industry and the federal government;

- Support the identification, monitoring, and reporting of complete, precise, and accurate challenges and hazards of health IT design and use;
- Incorporate telehealth and mobile health technologies and services within federal programs funding or providing health care and innovation model initiatives to improve access to and quality of health care services; and
- Improve the capacity of electronic information sources to support providers' ability to accurately and efficiently report and receive feedback on health care quality measures for public and private programs.

Despite our support for these and other listed strategies, we would encourage greater prioritization of the following issues in the near-term so that more substantive progress can be made toward long-term goals:

- Patient Matching;
- Cybersecurity in Healthcare;
- Sustainability of Meaningful Use;
- Patient Safety and Regulatory Oversight;
- Electronic Clinical Quality Measurement (eCQMs).

As policymakers look to develop an action plan based on this strategic plan, or as they consider program designs to help make progress against the numerous outcomes identified in the plan, we encourage all federal stakeholders to consider our recommendations listed in an appendix to this letter. CHIME continues to be grateful for the exceptional talent housed within all of our partner agencies and offices. Should you have any questions or require additional information, please contact Jeffery Smith, Vice President of Public Policy, at jsmith@cio-chime.org or (202) 507-6159. We look forward to a continuing dialogue with your offices on the realization of this Plan's stated goals.

Sincerely,

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

Charles E. Christian, CHCIO, LCHIME, FCHIME, FHIMSS
Chair, CHIME Board of Trustees
Vice President & Chief Information Officer
St. Francis Hospital

Attachment

College of Healthcare Information Management Executives
20 F Street NW, Suite 700 · Washington, DC 20001
Phone: (202) 507-6158 · Fax: (734) 665-4922 · staff@chimecentral.org · www.chimecentral.org

Below, CHIME articulates problem statements and offers recommendations to federal policymakers as they begin implementation of the Federal Health IT Strategic Plan.

Patient Identity Matching

Problem Statement: As exchange of health data becomes more commonplace, the accurate, efficient matching of patients with their data is a foundational component to interoperability and is a major threat to patient safety.

The challenge of accurately identifying patients and matching them with their data is not mentioned explicitly in the Plan. In fact, very little in the Plan can be construed to focus on record-linking positive patient identification or authentication. In Objective 2B: Identify, prioritize, and advance technical standards to support secure and interoperable health information, Strategy No. 3 is to "Advance technical and electronic methods to accurately identify, proof, match, and authenticate information across data sources." While CHIME supports this Strategy and overarching Objective, we are concerned that policymakers have somehow prioritized patient identity matching at the same level as provider authentication and online identity. Inaccurate patient identification is simply a much greater risk to the success of this Plan and the future of healthcare transformation, and it needs to be a top-level priority for ONC, HHS and the healthcare industry.

Recommendations:

1. HHS should improve patient identity matching through standardized data fields, and specifications should be included in the next Edition of Certified EHR Technology (CEHRT).

2. Pilot projects to demonstrate patient data matching strategies / solutions – including through unique identifiers – should be funded by HHS, NIST and other federal bodies.

Cybersecurity in Healthcare

Problem Statement: The digitization of personal health information (PHI) has led to an increase in the number and types of cyber threats facing healthcare. Meanwhile, providers lack a cost-effective, broadly-embraced national information-sharing infrastructure to discuss threats and they lack private / public incentives to proactively invest in cybersecurity technology.

Objective 2C of the Plan: Protect the privacy and security of health information includes two Strategies, one meant to help improve the cyber "stance" of the healthcare ecosystem and another meant to promote "bi-directional information sharing about cyber threats and vulnerabilities." There is growing consensus around the need to develop information-sharing networks that allow private sector actors to share information with the federal government and with their peers. Likewise, there is a need to have well-established networks for government officials to disseminate information out to the private sector. However, this is one side of the cyber equation; federal officials must also look for ways to better encourage and guide private sector investment in cybersecurity planning, threat mitigation and risk management. While the NIST Cybersecurity Framework is a great start towards the Strategy No. 1, the Plan does very little to address the challenge of investment in cybersecurity technology.

College of Healthcare Information Management Executives
20 F Street NW, Suite 700 · Washington, DC 20001
Phone: (202) 507-6158 · Fax: (734) 665-4922 · staff@chimecentral.org · www.chimecentral.org

Recommendations: 1. HHS should work with federal and private sector partners in continuing to develop a comprehensive set of usable guidelines, building on the NIST Cybersecurity Framework, to help providers mitigate cyber threats.

2. HHS should convene healthcare industry stakeholders to develop and promote industry-specific education materials and best practices for protecting health information from cyber criminals.

3. HHS should promote better cybersecurity information sharing between the private sector and government, and enhance collaboration and information sharing amongst the private sector.

4. HHS should provide targeted liability protection, safe harbor and legal deference for participating in information sharing networks and for proactively investing in improving the organization's cyber resiliency.

Meaningful Use

Problem Statement: The EHR Incentive Payments program is a vital driver of health IT, which sets a foundation for better population health, better healthcare delivery and lower costs. However, challenges with program implementation and future participation must be addressed.

While we appreciate the broad nature of the Plan to look beyond any one federal program, we are concerned that the federal government either does not believe Meaningful Use is a valuable policy lever to enact change within the industry or has decided it no longer deserves the priority it once garnered. CHIME has been and remains a staunch supporter of Meaningful Use and we envision a future where it is celebrated as a landmark program that helped move one of the nation's largest industries into the 21st Century. However, if this future is to be realized, the program must evolve and it must remain visible to federal leadership. We support Goal 1 in its entirety, but we urge rulemakers to reprioritize Meaningful Use, and ensure that other policies and programs support this innovation in policymaking.

Recommendations: 1. HHS should expedite plans to shorten the 2015 EHR reporting as indicated by CMS leadership.

2. CMS should allow providers the opportunity to demonstrate MU for a shortened reporting period during their first year of any new Stage.

3. CMS should address the "all-or-nothing" construct to enable more providers to continue program participation without receiving penalties.

4. In order to allow providers enough time to code, test, install, and optimize new functionality in CEHRT, CMS should allow providers three years at each Stage before being required to advance to a new Stage.

College of Healthcare Information Management Executives
20 F Street NW, Suite 700 · Washington, DC 20001
Phone: (202) 507-6158 · Fax: (734) 665-4922 · staff@chimecentral.org · www.chimecentral.org

5. Measures and Objectives for Stage 3 of the Meaningful Use Program should rely less on processes / thresholds and more on outcomes. All measures newly defined for Stage 3 and subsequent Stages should be electronically captured.

6. CMS must continue to find ways to harmonize quality measure reporting between various programs, including MU, Physician Quality Reporting System (PQRS) and the Inpatient Quality Reporting (IQR) program. Those required measures should be capable of electronic recording in the normal workflow while providing patient care.

7. ONC's Certification Program must be retooled to require more robust testing of EHRs to improve interoperability, ensure patient safety and to give providers confidence their certified products perform as advertised.

Patient Safety & Regulatory Oversight of Health IT

Problem Statement: As growing numbers of providers adopt health IT tools, patient safety is compromised by the lack of a robust event reporting infrastructure, the lack of process standards to develop, implement, maintain and retire health IT and market uncertainty over how new health IT functionality will be regulated by HHS.

CHIME supports Objective 1B: Increase user and market confidence in the safety and safe use of health IT products, systems, and services and its associated Strategies. We believe ONC and the wider federal government have an immensely important role to play in this area. However, we would encourage policymakers to work with private sector partners on the concept of shared responsibility, and the need to have a standard risk management process that covers the health IT lifecycle, including (1) design and development, (2) implementation and customization, and (3) post-deployment (including upgrades, maintenance, and operations, as well as surveillance, reporting, risk mitigation and remediation).

Recommendations: 1. HHS should provide financial and logistic / convening support for private-sector efforts to develop event reporting networks.

2. Similarly, HHS should support the development of a private-sector risk management process standard for ensuring patient safety throughout the health IT lifecycle.

3. To this end, a public-private partnership should be formed to develop an adaptable process for identifying standards and best practices, especially related to local implementation, customization and maintenance of health IT.

College of Healthcare Information Management Executives
20 F Street NW, Suite 700 · Washington, DC 20001
Phone: (202) 507-6158 · Fax: (734) 665-4922 · staff@chimecentral.org · www.chimecentral.org

4. HHS should encourage a legal environment that provides open pathways for users of health IT and patients they serve to report technology failures with implications for patient safety before such failures inflict patient harm.

5. HHS should not apply the medical device approval processes to functionalities considered part of health management or administrative software; rather, HHS should develop a sensible risk-based oversight framework with an emphasis on the end-users of the technology, including providers and patients.

Clinical Quality Measurement

Problem Statement: Several trends are converging to reduce fee-for-service reimbursement, but misalignments among quality reporting programs and technical barriers threaten the ability for policymakers to determine quality through electronic metrics.

The challenge of quality measurement is long-standing in healthcare, and recent advances in electronic quality measurement have complicated the task. Objective 2A, 3A and 3B all lean on the existence of accurate and complete quality measures as part of their underlying Strategies. We applaud federal lawmakers for highlighting the importance of quality measurement; however, we are concerned that leaders at HHS have given industry the "what" (harmonized measures, electronic reporting once and used multiple times) but there has been very little public discussion on the "how."

Recommendations: 1. Develop a common set of eCQMs across major reporting programs.

2. Establish a national test-bed for eCQMs so that providers can test their systems using in-house data to validate measures.

3. Allow submission of CQM data to qualified specialty registries as a substitute for quality program participation.

4. Focus more resources on the development of outcome-oriented quality measures.

College of Healthcare Information Management Executives
20 F Street NW, Suite 700 · Washington, DC 20001
Phone: (202) 507-6158 · Fax: (734) 665-4922 · staff@chimecentral.org · www.chimecentral.org