February 16, 2017

The Honorable Thomas Price, M.D.
Secretary, U.S. Department of Health & Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Secretary Price:

Congratulations on your confirmation as Secretary of Health and Human Services. We are eager to work with you and the department to pursue meaningful policies that enable providers to create a high-quality, low-cost healthcare delivery system. The College of Healthcare Information Management Executives (CHIME), which represents more than 2,300 health IT executives, strongly supports efforts to advance interoperability, reduce regulatory burden, improve cybersecurity, and more. CHIME members have moved beyond adopting information technology and to pursuing strategies that promote population health, patient engagement and value-based payment. However, significant barriers remain to harnessing the full power of these systems. Below are a set of priority areas and recommendations which, we believe, could propel us toward greater innovation in care delivery. A complete list of our recommendations can be found in the appendix. We thank you for your leadership in this area and look forward to continuing to remain an engaged partner.

1. **Patient Identification:** As our healthcare system moves toward nationwide health information exchange, we still lack the ability to identify patients with 100 percent accuracy 100 percent of the time. Errors in patient identification foster errors when it comes to matching patients to their medical records. Ultimately, this hampers interoperability, patient treatment, and patient safety. While a congressional ban prohibits HHS from spending funds on implementing unique patient identifiers, HHS should not be precluded from encouraging private sector efforts to locate a patient identification solution. CHIME in 2016 launched the National Patient ID Challenge, a crowd-sourcing challenge that aims to find a viable and scalable solution to ensure accurate patient identification. Addressing this problem is especially important as health information increasingly flows across unaffiliated providers in order to coordinate care and as patients




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

increasingly access and share their own data. Ensuring correct patient identification is the first step toward effectively protecting and securing identities and mitigating fraud. And, it is expected to save our system millions of dollars. **Our priority recommendation is for HHS to support private sector-ledefforts to locate a solution to patient identification and provide technical support.**

2. **Meaningful Use:** Born out of the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Meaningful Use program, now headed into its seventh year, has been very successful at helping hospitals and physicians achieve near universal adoption of electronic health records (EHR). However, it has failed to deliver the level of interoperability needed to facilitate seamless information sharing across different providers and has imposed a series of burdensome mandates on providers that increase the cost of care and often do not lead to better outcomes. Stage 3 implementation should be tied to a higher state of interoperability. **Our priority recommendation is for HHS to delay Stage 3 Meaningful Use requirements and use of Version 2015 CEHRT indefinitely while retaining a 90-day reporting period after 2017.**

3. **MIPS:** In order for payment and delivery reform to succeed, we need a high-performing, interoperable and secure technical infrastructure. Physicians and clinicians need ample time and interoperable EHRs in order to succeed. **Our priority recommendation is to treat 2018, in addition to 2017, as a transition year and remove the mandate to meet Stage 3-like measures under the Advancing Care Information (ACI) performance category of the Merit-Based Incentive Program (MIPS).**

4. **Interoperability:** Interoperability challenges continue to plague our health system to the detriment of patient care. Meaningful Use Stage 3 and Stage 3-like measures under MIPS required for use starting in 2018 demand a higher state of interoperability than currently exists. Yet, providers are being required to upgrade to a new version of certified EHRs (CEHRT) (Version 2015) that still cannot accomplish the level of interoperability needed. If providers are required to move to Stage 3 / Version 2015 CEHRT, they will not have a chance to benefit from the provisions outlined under the 21st Century Cures Act designed to improve interoperability. **Our priority recommendation is for HHS to prioritize the adoption of a single set of standards to facilitate interoperability.**

5. **Quality:** The complex web of quality reporting requirements not only create confusion among providers, but result in millions of dollars being wasted on creating cumbersome workflows, stealing time from direct patient care. On average, CHIME members are contending with submitting over 20 reports across federal, state and private sector programs each month, all with their own set of quality reporting requirements, oftentimes very similar, but nonetheless still sufficiently different so as to warrant different reporting workflows. Certified EHRs are ill-equipped to contend with reporting quality measures electronically, requiring additional costly investments by providers just to meet CMS requirements. **Our priority recommendation for HHS is to institute a 90-day reporting period for 2017 and beyond and to postpone reporting requirements of electronic clinical quality measures (eCQMs) until an appropriate technical infrastructure is in place.**

6. **Telemedicine:** The demand for parity in reimbursement for services provided in-person by a physician and those via telemedicine has never been greater. Medicare telehealth and remote patient monitoring reimbursement policies lag those of both state and private payers and thus needs to be expanded in order to achieve the transformational potential that widespread remote patient monitoring (RPM) and telemedicine adoption hold. Geographical limitations currently restrict the provision of telehealth services. The realignment of federal payment structures will be a key factor to increasing access to telehealth services to those patients who desperately need them. **Our priority recommendation is that HHS expand its coverage of telemedicine services and expand its coverage policies to support payment and delivery reform efforts.**


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

7. **Cybersecurity**: Cyber-attacks are highly disruptive or crippling to healthcare entities. Healthcare is deemed a critical infrastructure by the Department of Homeland Security and as such, patient safety and patient data should be viewed as a public good; protecting those things should be a national priority. Additionally, as payment and delivery system reforms propel us towards greater connectivity, new vulnerabilities arise. CHIME members take very seriously their responsibility to protect their systems and patient information, however, they face competing demands for limited resources – upgrading imaging and other clinical technologies, adopting health IT to comply with Meaningful Use, pursuing data analytics to support the move toward population health, and more. **Our top priority is for HHS to encourage investment in good cyber hygiene through positive incentives for providers.**

We appreciate the opportunity to offer you our ideas on bettering the healthcare system through the use of health IT and look forward to being a constructive partner in advancing this goal.

Sincerely,

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

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME


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

**APPENDIX**

| | | |
|---|---|---|
| **1.** | **Enabling the Use of a Healthcare-Specific Identification Solution** | |
| **1A.** | **Work with the private sector on locating a solution to patient identification** | We need a healthcare identification solution that, if stolen, does not have the same potential for fraud and abuse as the Social Security number. Recognizing that Congress must remove the language in the Labor-HHS Appropriations bill prohibiting HHS (in Sec. 510) from using any federal funds to "promulgate or adopt any final standard …. providing for the assignment of a unique health identifier for an individual," there is nothing in the law precluding HHS from offering technical assistance to private sector initiatives. Unfortunately, HHS has interpreted the annual funding ban to prohibit them from collaborating or assisting with private sector efforts to improve patient identification on a national level.<br>**Recommendation:** Encourage HHS to work with private sector partners who are taking the initiative to address patient identification, a critical issue to interoperability and patient safety. |
| **1B.** | **Encourage discussion** | The National Committee on Vital and Health Statistics (NCVHS) is the federal advisory committee that makes recommendations to HHS on all matters pertaining to the Health Insurance Portability & Accountability Act (HIPAA). While the congressional ban prohibits funding the promulgation of adoption of a standard, a robust dialogue around the challenges associated with patient matching and identification is not prohibited.<br>**Recommendation**: HHS should request NCVHS host a hearing on the topic of patient identification and matching. |
| **2.** | **Reduce Regulatory Burden of Meaningful Use Program** | |
| **2A:** | **Pause the program at Modified Stage 2** | Since MU began in 2011, various program requirements and stages have been delayed countless times largely due to the complexity. Providers and vendors have experienced a constantly shifting regulatory environment creating ongoing uncertainty and needless burdens.<br>**Recommendation:** Immediately pause the program indefinitely at Modified Stage 2 in order to allow the current program requirements to take root. |
| **2B:** | **Delay required use of Version 2015 CEHRT** | Providers are required to use certified EHRs (CEHRT) for MU and various other CMS programs. CMS requires providers under both MIPS and MU Stage to use Version 2015 CERHT beginning January 1, 2018, otherwise they face lower reimbursement. Yet, fewer than 1% of vendors have delivered Version 2015 products jeopardizing providers' ability to comply.<br>**Recommendation:** Indefinitely remove any mandatory use of Version 2015 CEHRT which is also needed to meet MU 3 measures. |
| **2C:** | **Remove the "pass / fail" approach to MU** | Current policy that punishes providers for even missing a portion of a measure is unnecessarily punitive and there is no evidence to suggest the current set of MU requirements have collectively resulted in better patient care.<br>**Recommendation:** Provide more latitude for providers to select the measures they feel best meet their patient's needs and they should only be required to have to meet 75% in order to be deemed successful. |
| **2D:** | **Institute a 90-day reporting period for all years** | For a variety of reasons, including but not limited to, upgrading systems or changing EHR vendors, providers are challenged to meet a 365-day reporting cycle.<br>**Recommendation:** The current 90-day reporting period should be maintained in perpetuity rather than mandating full-year compliance beginning in 2018. At the very least, the reporting periods for MU reporting period should be synchronized with the MU ACI reporting period which is 90 days through 2018. |


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

| | | |
|---|---|---|
| **2E:** | **Create a uniform set of requirements for all providers** | There are now three sets of MU requirements providers must navigate including one for Medicare clinicians under the Advancing Care Information (ACI) performance area of MIPS, another for Medicare hospitals, and yet another for Medicaid providers. Payment and delivery system reforms are pushing the industry toward a more coordinated delivery model. The complex web health IT reporting requirements will hinder providers' ability to focus on more coordinated care across the continuum. Today, providers must navigate three different sets of rules. Finally, Medicaid providers must meet an even higher set of thresholds than Medicare providers.<br>**Recommendation:** The different requirements under MU should be aligned such that all providers, no matter whether they are Medicare hospitals or Medicaid providers, are as similar as possible; requirements under ACI should also be as closely aligned to MU as possible; and Medicaid providers should not be unduly burdened by having to meet the most stringent set of requirements. |
| **3.** | **Modify MIPS Program to Maximize Physician Success** | |
| **3A.** | **Expand transition period** | CMS has declared 2017 a "year of transition." The changes under MIPS are substantial for physicians and sufficient time is needed to navigate the new system.<br>**Recommendation:** In order to give sufficient time to acclimate to the new system the transition period should be extended through 2018. |
| **3B.** | **Permanently shorten the reporting period** | CMS allows for a 90-day reporting period for Meaningful Use-like measures under MIPS but after 2018, a full-year begins. Several reasons may challenge providers to meet a full year, many outside their control.<br>**Recommendation:** Establish a 90-day reporting period for all reporting requirements in perpetuity. |
| **3C.** | **Delay required use of V2015 CEHRT** | Providers under Meaningful Use and MIPS are both required to use Version 2015 CEHRT starting January 1, 2018.<br>**Recommendation:** For the same reasons detailed under MU, the mandatory use of V15 CHERT should be delayed. |
| **3D.** | **Reduce quality reporting burdens** | Half of a clinician's score is derived from their quality measurement quality reporting.<br>**Recommendation:** Allow facility-based clinicians to elect to use their institution's performance rates as a proxy for the clinician's MIPS quality score |
| **3E.** | **Give credit for cybersecurity preparedness activities** | Small providers are particularly disadvantaged when it comes to having sufficient technical know-how and resources to guard against cyber threats.<br>**Recommendation:** Provide credit under the MIPS clinical practice improvement activity (CPIA) performance category for activities which improve a practice's cybersecurity hygiene. |
| **4.** | **Prioritize Interoperability** | |
| **4A.** | **Adopt a uniform set of standards** | A higher state of interoperability cannot be achieved without a uniform set of standards.<br>**Recommendation:** HHS should drive the identification and use of standards in priority areas to ensure providers are capturing and exchanging data in the same fashion. |
| **4B.** | **Streamline data blocking attestation statements** | MACRA calls on providers to attest they are not engaging in data blocking practices. CMS plans to require providers starting for the 2017 reporting year to attest to three statements, two of which go well beyond what is required under statute.<br>**Recommendation:** CMS should limit the requirement to the what is required under law which calls for attesting they did not "knowingly or willfully" impede interoperability. |


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

| | | |
|---|---|---|
| **4C.** | **Facilitate Interoperability Across the care continuum** | Too often, interoperability is considered something that needs to occur between doctors and hospitals. While there has been a steady and growing identified need to ensure patients have access to their data, there are major segments of the healthcare system where more concerted attention must be paid in order to ensure patient information is moving seamless across all providers and to support better care.<br>**Recommendation:** Increase efforts to ensure healthcare providers beyond doctor's office and hospitals (i.e. long-term care and behavioral health) are able to seamlessly exchange information such that care coordination is improved. |
| **5.** | **Streamline Quality Reporting** | |
| **5A.** | **Institute 90-day reporting** | Prior to 2017, there was a 90-day reporting period in place eCQMs. Beginning in 2017, CMS now requires a full year of quality data. CMS has said it is willing to consider shortening it.<br>**Recommendation:** Institute a 90-day reporting period as soon as possible for 2017 and retain this for future years. |
| **5B.** | **Halt mandatory electronic reporting** | Providers must use manual abstraction, a costly and cumbersome process, for gathering and reporting the measures to supplement electronically generated quality data, and this is likely to be the norm for some time to come.<br>**Recommendation**: Pause all mandatory reporting of electronic quality reporting mandates. |
| **5C.** | **Require fewer system updates** | The pace of change associated with eCQMs is outstripping provider and vendors' ability to keep up. Providers are faced with annual changes that put them in a constant state of upgrading.<br>**Recommendation:** Providers should not be required to make updates to their systems for quality measures any more than every two years. |
| **6.** | **Telemedicine** | |
| **6A.** | **Update Medicare's definition of telehealth** | CMS has taken steps to better utilize connected health technology in several components of Medicare, however, the pace of change is very slow.<br>**Recommendation:** Use rulemaking (i.e. Physician Fee Schedule (PFS)) and waivers to move away from antiquated reimbursement policies which largely preclude telehealth from being utilized in a meaningful manner and promote the use of remote monitoring technologies under CMS' existing authority. |
| **6B.** | **Expand coverage of telehealth for** | Under MACRA Congress directed CMS to embrace enhancements like connected health technology. The Clinical Practice Improvement Activity (CPIA) measurement category of MIPS could be expanded to better cover telehealth and connected technology use.<br>**Recommendation:** Expand the Medicare Telehealth Services List in the PFS rule and leverage CMS' Innovation Center to explore the benefits of new and innovative connected health technology. |
| **6C.** | **Support care coordination** | Medicare's reimbursement policies can be improved to better support care coordination.<br>**Recommendation**: Reimburse for non-face-to-face chronic care management services. |
| **6D.** | **Licensure** | Cross-state licensure concerns often imposing troublesome legal barriers to a physician wishing to offer telehealth services to a patient in another state.<br>**Recommendation**: 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 one's home should be considered. |
| **7.** | **Cybersecurity** | |
| **7A.** | **Incentivize security.** | Budgetary constraints can severely hamper a provider's ability to pursue sophisticated cybersecurity measures. Small providers are particularly disadvantaged. |


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

| | | |
|---|---|---|
| | | **Recommendation:** HHS should look for ways to encourage investment through positive incentives for providers such as those who demonstrate a minimum level of cyberattack readiness and mature information risk management programs, and those who make measure progress over time, including offering incentives under the clinical practice improvement activities of MIPS for practicing good cyber hygiene. To further enhance proactive collaboration, safe harbors from Resolution Agreements as an incentive for organizations that demonstrate, and certify, cybersecurity readiness should be offered. This will encourage the investment into cybersecurity from the providers in an age when it is understood no organization can prevent all cybersecurity attacks. |
| **7B.** | **Align privacy and security Policies** | The complexities with meeting HHS privacy and security requirements can be staggering. Audits by the Office for Civil Rights (OCR) are perceived as being punitive and not assisting the organization to recover and learn from a breach. Providers today have to dedicate highly valuable resources to navigate a complex and often unbalanced and punitive regulatory landscape.<br>**Recommendation:** HHS should:<br>1. Offer providers better guidance for assessing threats that they can control as opposed to those that are out of their domain;<br>2. Acknowledge and recognize provider efforts and investments to safeguard information and information systems when assessing the scope and magnitude of enforcement actions;<br>3. Offer more assistance to small providers;<br>4. Help providers maximizing protections allowed under business associates agreements (BAAs) by redistributing responsibility for security more evenly among covered entities and their business associates (BAs).<br>5. Set up town halls (virtual and or in person) to educate and to discuss key findings and lessons that can be shared and learned by all. |
| **7C.** | **Level-set security expectations for the healthcare industry** | Healthcare as a critical infrastructure is lagging in its preparedness to ward off cyberattacks.<br>**Recommendation:** In conjunction with federal partners, HHS should seek to develop a comprehensive set of recommendations building on the NIST Cybersecurity Framework, to help providers mitigate cyber threats and establish information risk management programs. Targeted liability protection should be extended to those participating in information sharing networks and meeting the expectations set forth by HHS. |
| **7D.** | **Workforce development programs.** | A workforce development program focused on healthcare cybersecurity, could leverage community colleges and professional certification programs to develop a skilled workforce to combat ongoing workforce shortages.<br>**Recommendation:** HHS should support ways to develop security experts to address both cyber concerns and general information security challenges. |
| **7E.** | **Improve the cybersecurity hygiene of medical devices** | The security of a device must be considered when evaluating the safety and efficacy of its performance.<br>**Recommendation:**<br>1) The Food and Drug Administration (FDA) should ensure that manufacturers configure their devices according to an industry accepted security standard that accounts for the basic principles of cybersecurity controls and alleviates risks;<br>2) Manufacturers should, as part of the pre-market approval process, be required to undergo a level of security validation in order to provide healthcare providers with a very simple and easy to implement mechanism for managing its security; and |

| | | |
|---|---|---|
| | | 3) Institute a clear enforcement process for reporting cybersecurity vulnerabilities that remain unaddressed by manufacturers.<br>4) Provide safe-harbor protections to manufacturers that follow the Food and Drug Administration's post market guidance on device cyber security, and penalties for manufacturers that fail to abide by the guidance in regards to uncontrolled risks. |
| **7F.** | **Increase transparency around device security** | Providers struggle to ascertain a device's security prior to purchase. In order for providers to be more informed consumers, greater transparency around device security capabilities is needed.<br>**Recommendation:**<br>1. Use and disclosure of the Manufacturer Disclosure Statement for Medical Device Security (MDS2) should be required in all procurement transactions in order to ensure transparency between manufacturer and HDO for a proper evaluation; and<br>2. Establish a database of FDA approved / cleared devices' security capabilities so that providers could have one-stop shopping and access to this information. This could be akin to the database overseen by ONC where certified electronic health record (EHR) vendors must report certain information on their products (aka the "CHPL" database).<br>3. Provide clear specifications (i.e. whitelisting) for any web links required for the proper function and use of a particular medical device. |