CHIME Response to the House Committee on Ways and Means
Medicare Red Tape Relief Project
August 25, 2017

Submission #1: Meaningful Use Program

Summary: The federal government has invested nearly $40 billion to spur the implementation and adoption of electronic health records across the nation. There's no question, with nearly all hospitals and the large majority of physicians participating in the Meaningful Use program, that the widespread implementation has been a success, but there is opportunity to reorient the EHR Incentive Program to better support patient care.

There is a growing amount of complexity as providers must manage three sets of program requirements: one for Medicare hospitals, an even greater set of thresholds for Medicaid providers, and finally an entirely different set of requirements for Medicare clinicians. This undue level of complexity is creating a drain on most hospitals. Recognizing that the Centers for Medicare and Medicaid Services (CMS) is bound by statute to carry out requirements that originate in different laws, we nonetheless believe there are opportunities to align program reporting more and reduce burdens on providers.

Related Statute/Regulation: The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

Proposed Solution:

Statutory Recommendation: Remove the requirement in the HITECH statute that requires the program to become more stringent over time, striking the below language as proposed in H.R. 3120.

> "The Secretary shall seek to improve the use of electronic health records and health care quality over time ~~by requiring more stringent measures of meaningful use selected under this paragraph.~~"

Statutory Recommendation: Congress should provide CMS the statutory authority, to align to the greatest degree possible, the three sets of Meaningful Use requirements – Medicare Hospitals (still in Meaningful Use), Medicaid Providers and Hospitals (still in Meaningful Use) and Medicare Clinicians (in Advancing Care Information under the Quality Payment Program).

Statutory Recommendation: Statutory changes should be made to immediately remove the pass/fail approach for Meaningful Use and eliminate the mandate to meet measure thresholds.

Regulatory Recommendation: CMS should permanently establish a 90-day reporting period, of the providers' choosing, for the Meaningful Use program and the Advancing Care Information (ACI) performance category.

Regulatory Recommendation: The Department of Health and Human Services (HHS) should undertake a systematic review of all Meaningful Use and quality measurement programs, soliciting provider and other stakeholder feedback on what is leading to better care and/or lowering costs.

Submission #2: Patient Identification

Summary: There is no standard for patient identification in the United States. Common practice today is to identify patients based on name and one or more personal identifiers, such as date of birth or street address and often Social Security Number (SSN). Unfortunately, name and date of birth offer no guarantee of accurate identification and often providers differ in how they record and store identifying information so other data elements, including how SSNs are leveraged. As patients visit multiple providers and records are exchanged, ensuring accurate identification is essential. With the growth of electronic health records, however, there is a greater risk of error if the bits and bytes do not match up.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 said, "The Secretary [of Health and Human Services] shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan and health care provider for use in the health care system."

The Congressional mandate for a unique health identifier was halted in 1998 by then-Representative Ron Paul (R-TX) with the insertion of a funding prohibition into the Department of Labor and Health and Human Services (Labor-HHS) appropriations bill, "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 (42 U.S.C. 1320d–2(b)) 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.[1]"

Ensuring correct patient identification is the first step toward effectively protecting and securing identities and mitigating fraud. It will also save our healthcare system millions of dollars. Further, our healthcare system will not be truly interoperable until patients can be correctly identified at the point of care.

Related Statute/Regulation: Health Insurance Portability and Accountability Act (HIPAA) of 1996; Sec. 510 of the Consolidated Appropriations Act 2017 (H.R.244)

Proposed Solutions:

Statutory Recommendation: Congress should remove or amend the federal funding prohibition that has contributed to the frequent use of SSNs to identify a patient.

> "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."

[1] Original Language - Section 516, Title V, Omnibus Consolidated and Emergency Supplemental Appropriations for FY 1999, H.R. 4328 (P.L. 105-277), October 21, 1998

Cybersecurity:

Summary: Cybersecurity attacks are highly disruptive and can be crippling to healthcare entities, as illustrated recently during the WannaCry and Petya ransomware attacks. The attacks impacted more than a dozen hospitals and countless other entities spanning the globe, reaching a reported 150 countries. 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.

Additionally, as payment and delivery system reforms propel us towards greater connectivity, new vulnerabilities arise. Given the growth in federal policies towards increased data sharing, many of which are rooted in Centers for Medicare and Medicaid Services (CMS), it is critical that cybersecurity remain at the forefront of policymaking rather than an afterthought. As such, policies are needed to help support providers secure their systems and patient data, and policies that reward good cyber hygiene should be developed.

Related Statute/Regulation: Health Insurance Portability and Accountability Act (HIPAA) of 1996; The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009; 45 CFR Parts 160 and 164 -- Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

Proposed Solutions:

Regulatory Recommendation: The Department of Health and Human Services (HHS), in coordination with the private sector, federal, and state partners, should look across HHS to harmonize regulations that directly or indirectly apply cybersecurity standards or best practices to reduce the burden on the industry.

Regulatory Recommendation: HHS should establish a conformity assessment model for evaluating cybersecurity hygiene that regulatory agencies and industry could rely on, instead of a diversity of auditors. The Office for Civil Rights (OCR) should establish consistent audit protocols across the industry rather than continuing the wide variation based on region and individual auditor.

Regulatory Recommendation: CMS should look for ways to encourage investment through positive incentives for providers such as: for as those who demonstrate a minimum level of cybersecurity hygiene and mature information risk management program, and those who make measurable progress over time. This should include an Improvement Activity under the Quality Payment Program (QPP) to reward clinicians who make investments to improve their cybersecurity posture and enhance privacy protections of patient data.

Regulatory Recommendation: CMS working together with the Office of the Inspector General (OIG) should expand safe harbors for donations of cybersecurity software, training and other tools helpful to small providers in fortifying their cyber hygiene.

Telemedicine

Summary: 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 need to be expanded 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.

Related Statute/Regulation: Section 1834(m) of the Social Security Act

Proposed Solutions:

Statutory Recommendation: Congress should clarify for the Department of Health and Human Services (HHS) that reimbursement for telehealth and other non-traditional care episodes must be accommodated and provide additional guidance on current telehealth reimbursement policies, including geographic and site limitations.

Regulatory Recommendation: HHS should engage in a national dialogue concerning the patchwork of state laws and licensure barriers impeding the expansion of telemedicine and remote patient monitoring.