American Hospital Association®

Health Information Technology

Background

The national transition to more integrated and patient-centered health care increases the importance of health information technology (IT) systems that allow clinical information and decision support to be deployed and shared widely and efficiently. The Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs provide incentives and penalties to encourage "meaningful use" of EHRs by hospitals and physicians. At the same time, hospitals and health systems are factoring other elements of health IT into their operations, including interoperability, cybersecurity and mobile health technologies. As with any new technology, health IT safety must be considered. For hospitals and physicians, all IT implementations also must be reviewed to ensure that they support the transition to ICD-10, which was recently delayed until Oct. 1, 2015.

AHA View

The AHA has been a longstanding advocate for health IT, specifically the rapid adoption of EHRs and national interoperability standards. Shared health information will allow clinicians and patients to have the information they need to promote health and make the most informed decisions about treatments. But this goal will be reached only if rules promoting IT adoption are clear and reflect the real-world practicalities of implementing new technology systems.

EHR Incentive Programs. In fiscal year (FY) 2014, all hospitals and physicians must upgrade to the 2014 Edition Certified EHR and meet higher performance requirements to qualify as meaningful users under Medicare and Medicaid. Hospitals paid under the inpatient prospective payment system face the loss of incentive payments and significant penalties if they cannot meet these requirements. Critical access hospitals also face the loss of incentives. Given the complexities of the program, and the delays in delivery of certified EHRs from vendors, the AHA, along with 47 other organizations, in late February urged the secretary of Health and Human Services (HHS) to extend through 2015 the timelines for hospitals, physicians and other eligible professionals to implement the 2014 Edition Certified EHR, and add flexibility in meaningful use requirements. With only a fraction of 2011 Edition products currently certified to 2014 Edition standards, it is clear the pace and scope of change have outstripped the ability of vendors to support providers. Hospitals are committed to implementing EHRs to support care improvements and patient engagement. They are investing capital and human resources to meet the meaningful use requirements and should be given the time needed to implement new technologies safely and effectively.

The AHA is very concerned that the fast pace and broad scope of the EHR incentive programs pose significant challenges to hospitals and physicians and will monitor progress carefully in 2014, with a particular focus on how smaller and rural facilities are faring. In addition, we will work with the federal government to ensure that any new rules, such as those that might be proposed for Stage 3 of meaningful use, are informed by field experience and carefully weigh the benefits of new requirements against the expected costs of compliance.

Supporting Physician Adoption of EHRs. The AHA is pleased that, in response to our advocacy, HHS issued a final rule that extended through 2021 the limited exception to the Stark law and the anti-kickback law safe harbor that permit hospitals to assist physicians in developing EHRs. Those protections were set to expire on Dec. 31, 2013.

Interoperability. As the adoption of EHRs spreads, hospitals and health systems are still constrained by systems that cannot efficiently share data across vendor products or departmental systems, even within an organization. Systematically sharing information across settings or organizations remains a big challenge. We expect increased interoperability that supports efficient information sharing to be a major focus of policy debate in the coming years. The AHA supports interoperability and will work to ensure that any new federal efforts to promote interoperability take into account how hospitals and physicians generate, use, share and secure health information, and the need for efficient solutions for information sharing among settings and with patients.

The issue of how to match patients with their medical records remains unresolved despite the continued push for interoperability on a national scale. The AHA continues to press for a resolution, and to recommend the creation of a nationally unique identifier system to connect records so that hospitals and physicians have the best information available when providing care for each patient. Such a system would facilitate efforts to increase the safety and quality of care given to patients.

The AHA is pleased that, in 2013, the Food and Drug Administration (FDA) finalized a system of unique identifiers for medical devices that will increase efficiency and add an element of transparency to the medical device industry by providing basic, standardized information on all medical devices. The unique device identifier (UDI) also will facilitate safety recalls and support improved quality of care. The AHA will work with members and FDA to ensure that the roll-out of the UDI is smooth, and encourage HHS to ensure that certified EHRs support the automated capture and use of UDI.

Cybersecurity. There is growing public and policy interest in ensuring that all information systems, not just those containing protected health information, are kept confidential and secure. In 2013, the White House issued an *Executive Order on Improving Critical Infrastructure Cybersecurity* with the goal of improving cybersecurity and reducing cyber threats to the nation's "critical infrastructure sectors," including the Healthcare and Public Health Sector, which includes hospitals. In 2014, the AHA continues to raise awareness of cybersecurity issues and risk management strategies. In particular, hospitals and health systems will want to understand the new National Institute of Standards and Technology (NIST) Framework on Cybersecurity. This framework provides a structure for organizing activities needed to manage cyber risks, such as identifying the cyber-security risks to systems, assets, data and capabilities; taking steps to protect against

them; and detecting and responding to any attacks that may occur. Compliance with the framework is voluntary; however, the federal government will be considering incentives to promote compliance in the coming years. The AHA offers numerous tools and materials for hospitals on cybersecurity, including webinars, suggested actions for hospitals and links to resources specific to the Healthcare and Public Health Sector. Visit *www.aha.org/cybersecurity*.

Mobile Health (mHealth). As hospitals and health systems adopt new technologies, so do consumers. Mobile health includes use of consumer-facing applications and technologies to manage personal health and promote wellness. Increasingly, health care providers are supporting consumer use of the technologies and considering ways to incorporate mobile health data into EHRs. At the policy level, the federal government is considering whether, and how, to regulate mobile apps to ensure safety, privacy concerns and technology standards that can facilitate the efficient flow of relevant information from devices to health care providers. In fact, the FDA recently issued guidance on mobile apps, and other agencies are expected to follow suit.

Health IT Safety. The increased use of EHRs has led to an increased focus on safety issues. It is the shared responsibility of health IT vendors, clinicians, health care organizations and federal agencies to ensure that health IT systems are designed, implemented and used to mitigate harm and promote safety. Steps to address safety should build on existing patient safety efforts across government programs and the private sector and address health IT as one of many factors affecting safety, rather than as a topic on its own. The AHA is pleased that the vendor community developed a voluntary code of conduct in 2013 that included specific commitments to ensuring and promoting safety. We will continue to push vendors for safe design and product development that will support safe use of their products. In addition, we will encourage vendors to remove from their contracts indemnity clauses or nondisclosure language that limits the ability of users to identify and raise safety concerns. Vendors also must increase transparency in pricing and adherence to existing coding conventions for systems that support billing. In 2014, we expect the federal government to produce a congressionally mandated report on health IT safety and the appropriate role of government in ensuring safety. For more information on safety issues, see the AHA's "Improving Quality and Patient Safety" issue paper.

ICD-10 Adoption. In 2009, HHS mandated adoption of new International Classification of Diseases (ICD) standards, or ICD-10. This replacement to the ICD-9 coding system was long overdue, and the AHA supports the change to ICD-10 because it provides greater precision in the classification of disease. The move to ICD-10 will mean better data to monitor resource utilization, improve clinical, financial and administrative performance and support biosurveillance of public health risks. The federal government has delayed the transition several times; most recently, Congress delayed the transition until Oct. 1, 2015.

The AHA opposes the recent one-year delay in implementation of the ICD-10 coding set. Many hospitals have incurred substantial financial obligations in implementing ICD-10, and this delay will slow down the transition to value-based payment in the health system. While the transition to ICD-10 entails significant challenges, ICD-10 will ensure payment accuracy and grow the nation's understanding of health care delivery.