



American Hospital
Association®

Maximizing Health Information Technology to Improve Care

AHA View

The AHA has long advocated for expanding the use of health information technology (IT), specifically the rapid adoption of electronic health records (EHRs) and national interoperability standards. Shared health information will allow clinicians and patients to have the knowledge they need to promote health and make the most informed decisions about treatments. This goal will be achieved only if the federal government cuts back on regulatory burdens and provides supportive policies. In addition, technology vendors must make data sharing across platforms easier for providers and consumers. For their part, hospitals must prioritize security of their information systems against cyber attacks.

Background

Hospitals continue to deploy robust health IT systems to support improvements in clinical care, efficiency efforts and delivery system transformation. Some of these changes were motivated by the Medicare and Medicaid EHR Incentive Programs, which provided a carrot-and-stick approach of incentives and penalties for hospitals and physicians that either meet or fail to meet the federal requirements of “meaningful use.” In addition to EHRs, hospitals increasingly are adopting telehealth, remote monitoring and data analytics solutions to expand the availability of care and improve coordination across care settings. While these technologies are essential for building the care system of the future, they can be expensive and unwieldy, and do not yet support the necessary level of easy information sharing expected by hospitals, other health care providers and consumers. Hospitals also are faced with a transition to the ICD-10 coding system on Oct. 1 and increased cyber threats from bad actors looking to disrupt information systems and steal data.

Key Priorities

The AHA will continue to work on several fronts to expand the use of health IT to improve health and health care. These include:

- Modifying the EHR incentive programs to include greater flexibility and improve electronic quality reporting;
- Implementing ICD-10 on Oct. 1, 2015, as planned;
- Increasing access to telehealth;
- Incorporating mobile health (mHealth);
- Improving interoperability;
- Implementing the Unique Device Identifier (UDI) in a responsible manner that enhances patient care;
- Maintaining cybersecurity; and
- Improving the safety of health IT.

Obtaining Greater Flexibility for the EHR Incentive Programs

The last Medicare EHR meaningful use incentives will be paid in 2016. Penalties under the program began in 2015 and do not sunset. About 200 hospitals are

receiving Medicare penalties in 2015, as are one of every two eligible professionals. The requirements of the program have been too prescriptive and burdensome, and hold hospitals and physicians accountable for the actions of others beyond their control. A recently released proposed rule would shorten the reporting period in 2015 to 90 days and provide flexibility on the patient portal requirements – key changes that the AHA has strongly advocated. The rule also introduces a host of other changes in the middle of the program year that could prove confusing and burdensome. At the same time, CMS has proposed new rules for Stage 3 of meaningful use that raise the bar too high once more, while lacking the flexibility hospitals need to succeed in the program and use IT to meet their own strategic goals. The AHA continues to advocate for a more reasonable timeline for the program, and greater flexibility in the requirements, building on successful advocacy efforts to increase flexibility in 2014.

Implementing ICD-10 in FY 2016

According to an AHA survey conducted in early 2015, 93 percent of hospitals are moderately to very confident that they will be able to meet the Oct. 1 start date for ICD-10, which Congress delayed by one year. Given the large investments hospitals and health systems have made in preparing for the transition to ICD-10, the AHA urges Congress to resist all calls to delay the start date yet again. A dual processing system allowing those who are not yet ready to use ICD-9 while everyone else uses ICD-10, as some have suggested, is unworkable.

Increasing Access to Telehealth

Telehealth is increasingly vital to our health care delivery system. According to AHA survey data, in 2013, 52 percent of hospitals utilized telehealth and another 10 percent were beginning the process of implementing telehealth services. As summarized in a recent AHA *TrendWatch* report, evidence is mounting that telehealth improves quality of care, expands access to needed services and meets consumer demands. The pace of technological change also makes new approaches possible, such as remote monitoring of patients and greater use of secure video visits. However, significant regulatory and legal barriers must be addressed for telehealth to fulfill its promise, including more rational approaches to physician licensure, clarity on e-prescribing and malpractice issues, and attention to how telehealth systems will be kept secure. The AHA strongly supports improvements in Medicare coverage and payment for telehealth.

Incorporating Mobile Health (mHealth)

Just as hospitals and health systems are adopting new technologies, so are consumers. Mobile health includes use of consumer-facing applications and technologies to manage personal health and promote wellness. Increasingly, health care providers, including hospitals and health systems, are supporting consumer use of such technologies and are considering ways to incorporate mHealth data into their EHRs.

Improving Interoperability

As EHR adoption increases, hospitals and health systems remain constrained by systems that cannot efficiently share data across different platforms or even across departmental systems. Systematically sharing information across settings or organizations remains a challenge. The AHA supports interoperability and is working to ensure that any new federal efforts, such as the “Interoperability Roadmap” drafted by the Office of the National Coordinator for Health IT, take into account how hospitals and physicians generate, use, share and secure health information, and the need for efficient solutions. The AHA continues to recommend the creation of a national unique patient identifier to better connect patient records so that hospitals and physicians have the best information available when providing care for each patient.

Implementing the UDI Responsibly

The AHA is pleased that, in 2013, the Food and Drug Administration (FDA) finalized a system of UDIs for medical devices that will facilitate safety recalls, support improved quality of care and improve efficiency. The AHA is working with hospitals and FDA to ensure a smooth roll-out of the UDI over the next six years, and encourage federal authorities to ensure that certified EHRs and registries support the automated capture and use of UDI. However, we have concerns about calls to require providers and payers to include the UDI on health care claims due to the large administrative burden and expense and unanswered questions about the UDI as a standard. Incorporating the UDI into EHRs and other clinical systems will bring the most benefit for patients.

Maintaining Cybersecurity

Hospitals and health systems have an obligation to keep all information systems, not just those containing protected health information, confidential and secure. In 2013, the White House issued the *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 health care and public health sector. In 2014, the AHA created a set of member education tools to raise awareness of cybersecurity issues and risk management strategies that is available at www.aha.org/cybersecurity. In 2015, we will continue these efforts and work with the federal government on its priorities, such as sharing information on cyber risks.

Ensuring the Safety of Health IT

Research has shown that health IT can both improve safety and introduce new risks for patients, raising the question of what is the appropriate role for government in overseeing health IT safety. The AHA believes that 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. On a policy level, the AHA wants to ensure that federal safety oversight for health IT is nimble but sufficient to protect patient safety, and that hospitals and other providers are not exposed to liability from unsafe products.