VIEW FROM THE TOP

DeSalvo: Health IT Is ‘More Than Just EHRs’

Let’s start by looking at the overall mission of your office. Encouraging the adoption and use of electronic health records is clearly a priority. How else would you describe the overall vision for the ONC?

ONC was created in 2004 by President George W. Bush to help expand the use of health information technology (IT) across the country. Over the past 10 years, thanks in great part to the enactment of the HITECH (Health Information Technology for Economic and Clinical Health) provisions in the American Recovery and Revitalization Act (ARRA), we have passed the tipping point in the adoption of health IT and electronic health records (EHRs). But health IT is more than just EHRs, it is the broader use of health information technology to help improve the nation’s health. While meaningful use creates the foundation for interoperability, it is now time to move beyond MU to drive interoperability across the care continuum by marrying standards to federal policies that will facilitate many different types of exchange over the next several years to meet the demands of delivery system reform. To drive this, ONC is focusing on five streams for effort:

• Adoption and Optimization of EHRs and health IT
• Standards to Support Implementation and Certification
• Financial and Clinical Incentives
• Privacy and Security
• Rules of Engagement or Governance

In 2014, you announced a reorganization at the ONC. Can you explain its purpose?

The HITECH grant programs—the Beacon Communities, the regional extension centers, and the state health information exchange organizations—are ending, and we fully expected that the agency would be restructured to meet the expectations of the nation for the next chapter of work. So, as an organization, we are pivoting from a focus on those grant programs and adoption through the Medicare and Medicaid EHR Incentive Programs, to serve as coordinator for health IT across the administration and with the private sector. ONC will continue to serve as the convener to advance health IT and innovation with the aim of enabling and informing health delivery reform and improving the public’s health. ONC will also leverage its existing authorities and responsibilities to advance health information technology to facilitate coordinated care and improved outcomes. We will continue to increase the focus on payment and delivery reform, improve our EHR certification process while expanding it to include other types of providers—such as behavioral health and long-term, post-acute care facilities, engage stakeholders through Federal Advisory Committee Act (FACA) committees, and much more.

Karen DeSalvo is a physician and public health expert who serves as the National Coordinator for Health Information Technology and director of the Office of the National Coordinator for Health Information Technology (ONC), a division of the U.S. Department of Health & Human Services (HHS). DeSalvo was tapped to serve as acting assistant secretary of health to lead HHS’ public health efforts, especially its response to the Ebola virus outbreak.
and work with our partners on the ground. We will also be looking at ways to further engage patients, through education of ways to leverage health data and new technologies that will enable them to use health IT to improve their health, their care, and lower their healthcare costs.

You were at the forefront of efforts to modernize healthcare in New Orleans following Hurricane Katrina. How can the lessons you learned there translate to a national level, particularly as it relates to healthcare technology?

New Orleans is indeed a laboratory for innovation, including in health IT. One of the many ways our experience in New Orleans can translate to a national level is the collaborative spirit we formed around health IT as part of the Crescent City Beacon Community, an ONC grant program. Partners and stakeholders who were disparate, even competitors, came to the table to talk about ways to improve the health of our community and using every tool at our collective disposal to do so. I think the nation can learn much from communities like New Orleans that put interests aside to do the right thing for the public’s health.

How important do you think your hands-on experience in Louisiana is to your effectiveness in your current post?

My experience in Louisiana has shaped me personally and professionally. I understand intimately what it is like to build an efficient, neighborhood-based, high-quality healthcare infrastructure from the ground up, in a devastated community. And the importance of health IT as a necessary component to do so. To your point about “hands-on” experience, I also understand what it is like to be a doctor and practice medicine in this environment. I think both of these perspectives help me to lead our efforts without losing sight of what is important on the ground.

AAMI members include clinical engineers and biomedical equipment technicians, all of whom take care of medical devices and technology in healthcare facilities. How do you see their roles changing as IT becomes such an integral part of healthcare in general?

These devices have started to format data in a way that is easily ingested by EHRs. This is actually a key component of what Integrating the Healthcare Enterprise (IHE) has been focusing on. We expect that the roles of these devices will become more and more integrated into the delivery system. The sharing of data—patient generated data to data generated by these devices—is already making improvements in health.

What’s the most important thing these professionals can do to help their facilities improve the delivery of healthcare and the overall patient experience?

The most important thing they can do is to help ensure that information can be shared at the right place and the right time. They should not create islands of automation, but instead help to ensure that information is interoperable.

What about medical device manufacturers? As more devices and systems connect to one another, do you have any thoughts on how they should approach the development of new products?

Try not to create islands of automation in the way that early imaging modalities did.

What do you see as the single biggest challenge as it relates to health IT?

One of the greatest challenges is achieving a nationwide interoperable health IT policy and technology framework that helps to collect, use and share data to improve the health and care of patients while lowering costs. This is important because health IT is a fundamental component of new payment and delivery system models, which rely heavily on information sharing across practices and health systems. By moving from a reimbursement system that pays providers for volume of treatments to a
system that pays for the quality of care, providers will see benefits in using health IT to manage information about their patients. In its role as a convener of the health and health IT industries, ONC is looking at how to leverage other HHS and federal programs, resources, and policy levers to promote interoperability and information exchange. The near-term goal is to develop and implement a set of policies to encourage providers to exchange and seek health information routinely through interoperable systems in support of care coordination across healthcare settings. Most importantly, health IT can help clinicians improve the quality and safety of care provided to patients, through a wide range of electronic tools, such as:

- Accessing up-to-date evidence-based clinical guidelines and decision support
- Providing better proactive health maintenance support for patients
- Better coordinating patients’ care with other care providers through the secure and private sharing of clinical information.
- Engaging patients to be part of the care team by implementing Blue Button capabilities that give patients access to their health information.

There seem to be a fair number of hotly debated topics in healthcare IT. What is one topic that you wish had immediate across-the-board support, and why?

It seems that the nation’s priorities are well aligned with the expectations of consumers. To be clear that we have the right set of priorities, ONC is leading the renewal of the Federal Health IT Strategic Plan and we will seek public comment until Feb. 6.

One hurdle to true interoperability would appear to be the fact that healthcare has not yet fully embraced systems engineering principles compared with other industries. Would you agree this is a factor? Why?

One of the challenges is that in other industries large components of the workflow are dominated by one vendor, or at least within a business deployment. When someone installs an energy system from GE, it is systemwide and doesn’t have to talk to the business next door. Further it doesn’t talk to the elevators, or the computer infrastructure, etc. There aren’t many examples of industry systemwide interoperability. In the end, it is a tough problem.
Another challenge to interoperability would be a lack of standardization. Is the ONC doing anything on that front?

Core technical standards is one of the building blocks to achieve a nationwide interoperable health IT infrastructure. Through our Standards & Interoperability Framework, we will continue to work closely with all of the stakeholders, including members of AAMI, to advance core technical standards for terminology and vocabulary, content and format, transport, and security.

There aren’t many examples of industry systemwide interoperability. In the end, it is a tough problem.

What about the alignment of incentives when it comes to interoperability? How can ONC help?

Again, this is another building block in achieving the goal. While the Medicare and Medicaid EHR Incentive Programs have been a primary motivator for the adoption and use of EHRs, we need to move beyond thinking that health IT is only EHRs. Current policies and financial incentives often keep the exchange of health information from happening, even if it is technically possible. We need to migrate policy and funding levers to create the business and clinical imperatives—the incentives, if you will—for interoperability and electronic health information exchange.

No information technology system is completely secure, even with multiple security controls. Threats and vulnerabilities are always (and rapidly) evolving. Healthcare providers should make sure that the applicable security controls and safeguards are in place based on a risk assessment of their particular environment. The best practice is that risk assessments are a continuous process. HHS’s Office of Civil Rights “Guidance on Risk Analysis Requirements under the HIPAA Security Rule” also states that the risk assessment process should be ongoing. The NIST Cybersecurity Framework (released in Feb. 2014) uses standards/guidelines/industry best practices on cybersecurity risk management and how to incorporate cybersecurity into an organization’s current and existing information security program. It provides a starting point for our stakeholders as they think about addressing cybersecurity risks within their environments. It also offers a methodology that aligns with existing incident management best practices and frameworks. We are continuing to offer information to providers and other stakeholders about ways to protect electronic health information and health IT and specifically emphasizing the relevance of cybersecurity risks to the healthcare environment. That includes encouraging them to use and adopt NIST’s framework, based on their specific business needs and existing organizational policies and security programs. It is also important for providers to know how the Framework relates to the HIPAA Security Rule requirements.

Another big topic is cybersecurity. How vulnerable are hospitals to both breaches in patient data and to the actions of hackers who might cause specific devices or systems to malfunction?

No IT system is completely secure, even with multiple security controls. Threats and vulnerabilities are always (and rapidly) evolving. Healthcare providers should make sure that the applicable security controls and safeguards are in place based on a risk assessment of their particular environment. The best practice is that risk assessments are a continuous process. HHS’s Office of Civil Rights “Guidance on Risk Analysis Requirements under the HIPAA Security Rule” also states that the risk assessment process should be ongoing. The NIST Cybersecurity Framework (released in Feb. 2014) uses standards/guidelines/industry best practices on cybersecurity risk management and how to incorporate cybersecurity into an organization’s current and existing information security program. It provides a starting point for our stakeholders as they think about addressing cybersecurity risks within their environments. It also offers a methodology that aligns with existing incident management best practices and frameworks. We are continuing to offer information to providers and other stakeholders about ways to protect electronic health information and health IT and specifically emphasizing the relevance of cybersecurity risks to the healthcare environment. That includes encouraging them to use and adopt NIST’s framework, based on their specific business needs and existing organizational policies and security programs. It is also important for providers to know how the Framework relates to the HIPAA Security Rule requirements.

Let’s move on to another subject: Big Data. That appears to be one of the hottest buzzwords in healthcare right now. Do you think there’s a danger of too much data being generated, but too little knowledge? In other words, is the right data being collected and analyzed, and are the right people connecting the dots? If not, how can healthcare turn data into knowledge?

The White House recently released a report on Big Data and Privacy that nicely describes the opportunities and challenges. We participated in that process and will be charged with working on the privacy issues in partnership with the private sector.
What should healthcare facilities be doing to address this challenge?

Healthcare organizations are strongly encouraged to evaluate and incorporate the requirements and guidance offered by the Cybersecurity Framework in the context of their specific environment and information security requirements. Their patients rely on them to keep their information safe and secure. Given that there are many federal and state regulations imposed on healthcare organizations, including HIPAA, we also encourage them to adopt (overlay) the framework in their own existing organizational policies and frameworks. We’ve been talking about various challenges through the lens of healthcare, regulator, and industry professionals. But the movement of more healthcare into homes and other non-controlled settings introduces a whole new wrinkle to the challenges associated with modern healthcare. What do you worry about as you see that evolution unfold? I only worry that we need to develop a policy and technology framework that can better support that type of care, convenience, and independence. We are working to achieve that.

The delivery of modern healthcare seems increasingly complicated. Is there one rule of thumb that all stakeholders—whether hospitals, industry, regulators or even patients—should keep in mind when considering how to best navigate it?

That we have one customer, one boss. The people of America. If we keep them at the center, it will help make our decision making and prioritization easier.

Sphygmomanometer Collection

Just updated, this collection is your single source for current Sphygmomanometer standards.


Order Code: 81060-S or 81060-S-PDF
List $300 / AAMI member $180

Order Your Copy Today! Call 877-249-8226 or visit http://my.aami.org/store