Doctors Face Conflicting Standards of EHRs

BY MARY ELLEN SCHNEIDER
Senior Writer

BOSTON — Interoperability is key to the success of electronic health records, but there are barriers to sharing data between systems, said David Brailer, M.D., national coordinator for health information technology.

The major challenges include standards harmonization, unclear data control policies, a lack of uniform security practices, the inability to ensure that products perform as advertised, and the lack of a business model around interoperability, he said.

"At the very basis of this—kind of the DNA of the interoperable electronic health record—is the emergence of harmonized standards," Dr. Brailer said at a congress sponsored by the American Medical Informatics Association.

Many organizations are involved in developing and approving standards, but there isn't a process for harmonizing two conflicting standards, according to Dr. Brailer.

In addition, there is no unified maintenance or release schedule for standards so that the industry can know what's coming and build investment plans around it.

Further, there is no means of providing input into the standards process, he said. For example, there isn't a mechanism for taking a problem and distilling that into requirements that could be used by organizations that develop standards.

"Problems don't come well packaged into a standard," Dr. Brailer said.

Harmonized standards are at the core of interoperability, but even with standards there are many other factors in achieving interoperability, he said.

One less well-known obstacle to interoperability is the lack of clear policies about data control. Health care right now lacks even a vocabulary to talk about the control of data, Dr. Brailer said.

Deciding on a set of terms and their meanings will be essential to figuring out who decides if information flows from point A to point B, in what way, and who will be notified.

Security standards pose another set of problems, Dr. Brailer said. Currently, it's possible for any two health care organizations to be compliant with the Health Insurance Portability and Accountability Act of 1996 and still have security practices that render their data unable to be shared.

For example, one organization may adopt user names and passwords for authentication while another organization uses a biometric thumbprint.

Some solutions are being developed to bridge the different levels of security. For example, security brokers or other third parties could navigate between two systems. And some states have talked about creating more requirements for uniformity of security practices.

Challenges include standards harmonization and unclear data control policies.

DR. BRAILER

"I think this is a profound barrier to our ability to be interoperable, and standards won't address it," Dr. Brailer said.

Physicians also need to be able to know if the system they purchase will be able to deliver on the vendor's promises of interoperability. The industry is taking a step in that direction with the formation last year of the Certification Commission for Healthcare Information Technology, a group that will certify that EHRs and other products meet minimum standards.

This work is important not just so that EHRs will one day become "plug and play" technology, Dr. Brailer said, but also because it will take some of the risk out of the marketplace.

But ultimately, interoperable EHRs can't become successful without a viable business model. The industry is just starting to experiment with the value drivers in this area, such as research, clinical improvement, and transaction simplification compared with paper.

"The government's not going to tell you what the business model is," Dr. Brailer said.

The challenge is not just what the business benefit is but who receives it, he said. And Dr. Brailer predicts that this interplay of costs and benefits will lead to new relationships between providers and payers and other entities. ■