

Paul Connelly
Vice President and Chief Information Security Officer
Hospital Corporation of America

HIT Standards Committee Meeting
November 19, 2009
Washington, DC

Scope: Systems Stability and Reliability Panel – security challenges related to maintaining the stability and reliability of EHRs in the face of natural and technological threats.

Thank you for the opportunity to participate in this discussion. This is an exciting time to be in health care, and the opportunity to make a difference for our patients through the wise use of Information Technology has never been greater.

Hospital Corporation of America embraces the objective of the implementation and meaningful use of Electronic Health Records, and we are hard at work on that goal. At the same time, we are hard at work on ensuring that privacy and security are baked into those systems.

President Obama recently called cyber threats one of our "most serious economic and national security challenges." As you all know, security in a health care environment is a delicate balancing act between ease of use, cost, and risk; and delivery of patient care trumps other considerations. As a health care provider, HCA is facing the serious challenge of protecting our patients and our systems, and trying to remove obstacles to access for physicians and clinicians, at the same time our IT budgets are being squeezed and compliance demands are increasing.

Privacy and Security are essential elements of stable and reliable use of an Electronic Health Record. As patient records move to electronic format, and then are exchanged between different entities in the health care chain, both the providers and the patients have to have confidence that this sensitive information will be available to the people who need it, will be available when they need it, and it will be accurate and complete.

Exchange of data creates an *ecosystem* where we are only as strong as our weakest link. If we are going to exchange EHRs with other providers and entities in the health care chain, we have to have confidence in the Health Information Exchange and the other entities' ability to protect that data. Loss of confidence in the confidentiality, integrity, or availability of the data at any point in the chain could be the undoing of an EHR system, and it is critical that we ensure reliability and stability.

We applaud the efforts of this committee to identify the applicable standards for security and privacy. One could argue that security and privacy are the lynchpins that facilitate the success of Electronic Health Records and a Health Information Exchange. When a provider shows they

have met requirements for maintaining Confidentiality, Integrity, and Availability, they can use and exchange EHRs. Consistent implementation of standards will facilitate that trust in the confidentiality, integrity, and availability of the records and will create the reliable and stable “ecosystem” necessary for success.

Based on our reading about the progress of the Privacy and Security Workgroup and this committee, we feel the effort is on the right track. Establishing standards, implementation timelines, and certification criteria in each of the key areas you have identified will help all of us know “what” needs to be accomplished and “when.”

Right now, I would describe our organization as being in the mode of trying to understand the “what,” so in turn we can ensure we have identified and implemented the correct “How” we do it.

As practitioners focused on implementing and maintaining privacy and security standards as part of our EHR efforts, I’d like to call out four areas where your actions could help facilitate our efforts:

- Clear implementation guidance. On the provider side alone, there is so much variation from one entity to another, it is essential that guidelines for implementing privacy and security standards be clear. Because we operate 170 hospitals, HCA has a substantial amount of resources (more than 80 people) 100% dedicated to information security, and that scale gives us capabilities that our colleagues at neighboring hospitals just don’t have. Because we want to have a stable, reliable, and secure exchange of health information with those entities we need clear implementation guidance to put us all on equal footing.
- Setting priority for scarce resources. The incentives tied to EHRs have providers, product companies, and consultants off-to-the-races to plan for deployment and meaningful use of EHRs. Clear direction on how security and privacy are linked to receiving incentives and how we demonstrate our compliance will keep privacy and security an integral part of EHR efforts.
- Security being built into health care IT products. On the provider side, it seems the HIPAA security rule put the onus on us to drive vendors to provide compliant products through market demand. This has largely not happened, in my view. Our market demand for secure products has not driven health care IT product vendors to develop and deliver secure products. Although improvements have occurred, seven years after HIPAA, even the leading vendors of health care IT products today are selling systems to our hospitals that do not meet basic security standards set by the HIPAA Rule. I request you consider how standards can be used to drive the implementation of security measures into health care IT products though means other than market forces.
- Dealing with new risks. Meaningful use of EHRs creates new risks for provider organizations and our patients. There are other new developments, such as cloud

computing for example, that create other new risks. Direction and guidance for addressing these issues will create important consistency across the EHR ecosystem.

In summary, we are committed to doing the right thing, and actions by your group can help us understand exactly what the “right thing” is and help guide our actions. The clearer the guidance, the less room for interpretation and variation—the more you can facilitate the meaningful use of stable and reliable EHRs and benefitting and protecting the patients we serve.

Thank you.

Paul Connelly
Vice President and Chief Information Security Officer
Hospital Corporation of America