Interoperability, Standards, and Security
Program Transcript

[MUSIC PLAYING]

NARRATOR: To maximize the benefits of informatics for the health care community, various health information systems must be able to communicate efficiently and securely. Dr. Stuart Speedie, Dr. Ken Majkowski, and Dr. Donald Rucker describe challenges of information exchange and identify standards that are guiding the industry toward greater interoperability. And Stephanie Reel outlines steps organizations can take to safeguard sensitive clinical and administrative information.

STUART M SPEEDIE: A provider of health care, regardless of where they are located, if they have to take care of a patient they should be able to have access to all of the relevant information about that patient or to make the best possible medical decisions for the patients. The patients are taken care of in a variety of different settings. They may go to their primary care physician for most of their basic care. That primary care physician maintains-- in these days, we hope-- an electronic medical record.

If they are in an auto accident, they will go to the hospital or the emergency room. And they might well get admitted to the hospital. Then they become part of another electronic medical record system in the hospital.

They may need to have outpatient surgery at some point, perhaps by an orthopedic surgeon, in order to repair the damage as a result of that accident. If that takes place in a surgery center, then there's another medical record that's being created for that patient.

Now ideally, all of those different electronic medical record systems at the various locations should be able to share the information about the patient. And so from those various sources you build a complete and coherent picture of the patient's medical condition based upon the observations and reporting of all of the professionals involved. So that's the goal that we're trying to do.

The hows of doing it-- that turns out to be a much more interesting and admittedly difficult situation involving focusing on standards, on how we have standards for information exchange, and how we also set agreements to protect privacy, and how we secure that information, and how we make sure that it doesn't go to the wrong parties in that kind of exchange of information. So all of those factors come into play when we think about, if you will, exchanging information between hospitals.

We tend to think of an electronic medical record as a single system. In most health care organizations, there are many such systems. And some might
Interoperability, Standards, and Security

support the radiology department and storing and transmitting x-rays. Others might support the pharmacy department in terms of keeping track of medications.

There’s a whole host of those systems. Those systems have to also communicate with each other in order to do the kinds of information exchange within an institution. There, it’s a matter of working with the different vendors and making sure that there are proper standards in place so that the information that is generated by one system is able to be understood by the system that's receiving it and vice versa. And that's really the key when we talk about the notion of interoperability.

KEN MAJKOWSKI: Can one system talk to another system? Can many systems talk to many other systems? Interoperability has a lot of different meanings.

And it really needs to be phased in over time. So when we talk about interoperability in e-prescribing, we're able to get, for example, payer data in real time to a physician's application so that decisions can be made about the prescription.

We can also talk about interoperability of that same physician's application able to transmit that prescription to literally 47,000, 48,000 pharmacies across the United States, wherever that patient might want that prescription transmitted, and to do all of this electronically. We can take an electronic prescribing interoperability to the next step and say, is that e-prescribing application interoperable with the patient's electronic medical record?

So when the physician writes the prescription to be sent electronically, does that same prescription then go into the electronic medical record, so that it's documented that that patient had that drug prescribed? And then even take it a little bit further. If it's an enterprise system, that system is being used not only in a physician's office but maybe in a hospital system as well. Because that physician is employed by that hospital system. When that patient is admitted to the hospital, are all those records then available to the hospital system when the patient is being treated there as well?

So we can continue to take interoperability even further. Now that it exists in that patient's EMR, when that patient is being seen in a different hospital system across town, can it be transferred to a different hospital system? And that's what health information exchanges are attempting to do.

And to take it even further, the national health information network which has been proposed is, let's take the patient who is being seen by a physician and has information in their EMR in St. Paul, Minnesota, but is vacationing in Phoenix, Arizona and needs to go to an emergency room in Phoenix, Arizona. How fast can you get that patient's records to that emergency room in Phoenix, Arizona?
Now we're really starting to talk about true interoperability. It's not just a single system talking to a single system, but a system being able to talk to all systems.

[MUSIC PLAYING]

There are many challenges to interoperability. There are many moving parts. The way to try to overcome some of those obstacles is by using technical standards. And people are saying, are there standards for the delivery of this specific information?

In electronic prescribing we're very, very lucky. We have some very good technical standards that have been in use for six or seven years. They have been tested in CMS e-prescribing pilots-- there's five different pilots-- in the late 2000s. And these pilots have looked at the standards and said, yes. These are practical and useful and appropriate standards for e-prescribing.

Now if we think about interoperability of all medical records, we have to start talking about technical standards for laboratory, for imagery, for documentation, for a variety of things. And all those are being worked on by various committees and organizations, both government and private, across the country. In e-prescribing there is a standards organization referred to as NCPDP, or the National Council for Prescription Drug Programs, which has created technical standards for the pharmacy industry.

So we use something called the NCPDP script standard to transmit things like medication history and electronic prescriptions between physicians and pharmacies and between payers and physicians.

DONALD W RUCKER: We're talking about extraordinarily complex biological workflows. And in those very complex workflows, can you represent everything uniformly, let's say, in just the United States? And the answer to that, somewhat obviously, but somewhat not obviously, is probably not. Right?

There are simply so many differences. That is not a simple thing to automatically say, everything will interoperate. Hospital software is about embedded workflows. Office medical software is about embedded workflows.

All enterprise software is about embedded workflows, no matter what you have. And so your degree of interoperability-- your degree of standards-- have to reflect on some level the richness of those embedded workflows. There are some areas that we have clearly been able to very successfully standardize.

And so if you look at standards out there now-- for example, HL7, Health Level 7, is probably the workhorse standard for clinical communication. So if you're doing lab ordering and lab result transmission, those would be HL7 standards. And radiology and radiology information systems and PACS systems-- again, the
Interoperability, Standards, and Security

Picture Archiving and Communication Storage— the DICOM standards, D-I-C-O-M, that have been a combination of the radiology community and the National Electrical Manufacturers Association— so the manufacturers of this equipment— have been very successful standards.

And then of course all these sit on the wire standards. And those are the ones you know— internet protocols, HTTP. Those are the basic ones that are out there. Now there are some richer standards being developed—for example, the Continuity of Care Documentation standards that are part of the HITSP, the Health IT Standards Program that Health and Human Services has funded. Those standards are currently evolving.

So that’s standards to allow sharing of medical problem lists and medication lists and allergy lists. So they’re an evolution. They’re of course richer standards. Because as you might imagine, the name of disease might not be exactly the same for everybody.

So congestive heart failure might be one person’s idea of heart failure. Somebody else may subcharacterize congestive heart failure into diastolic failure and systolic failure. A cardiologist may subcategorize congestive heart failure into exactly what the valve is, what the etiology is, and what the ejection fraction is.

Well it sounds like it’s one disease. But they’re really very different levels of characterization. So the communications you build up— these richer standards— is a challenge.

[MUSIC PLAYING]

STUART M SPEEDIE: When we talk about the exchange of information between organizations, there are a number of legal ramifications in addition to the technical ramifications of simply moving information from one system to another. And those legal ramifications are actually governed, first of all, by the HIPAA regulations— the Health Information Portability and Accessibility Act that was passed about a decade ago. And that has subsequently been updated by the ARRA or the stimulus bill. That has changed some of the components of that regulation.

But fundamentally, what that says is that each organization has a legal responsibility to protect the information of that patient and to assure its appropriate use, regardless of where that use might be. As a result, it’s not simply a matter of exchanging a data file from one organization to another. The organizations have to have a legal agreement between themselves in order to exchange that information to make sure that the patient is properly protected. So that adds another layer onto the technical issues of information exchange.
STEPHANIE L REEL: One of the responsibilities that information technology professionals have-- and in particular CIOs have-- is to protect the assets of the organization. And those assets may include financial information, administrative information, or in our case, they certainly include patient-related information. And we take the protection of those assets very, very seriously.

We know that our patients trust us with the most sensitive information about their life and death experiences, life-altering experiences. They trust us with their health. And they trust us with their health information.

Several years ago, Johns Hopkins was cited for a theft of clinical information. A couple of workstations were stolen from our campus. And they included on them clinical information associated with a clinical research protocol.

After many, many, many hours stressing over what could have been and should have been done differently, we developed what we fondly came to refer to as a 12-step plan for how to protect information that resides on workstations, resides on portable media, as well as fixed media-- to ensure that we were doing everything possible to protect our patients and to protect the information assets of the organization.

Our 12-step plan can be easily boiled down to three components. We said, first and foremost, we will educate. We will educate the user community as to the risks associated with this huge repository of information that they have the ability to help manage and maintain.

The second step was another E. It was the E of environment-- that it was everyone's responsibility to create an environment that was conducive to privacy and security. That meant we would each allow ourselves to be held accountable for the environment within which we work.

So that may be physical security. It may be virtual security. It may mean that as we share information with others, we take great pains to ensure that it is shared appropriately.

It means that we would create less paper. Because paper has its own set of vulnerabilities. So we encouraged less printing of information.

And the third E was a very tactical one. It was encryption. So education, environment, and encryption became the three legs of our stool, if you will, associated with information security.

So we embraced a very aggressive program associated with encrypting information. So information that would reside on any portable device would be encrypted. So should it be misplaced, lost, or stolen, there'd be a great deal of difficulty in anyone being able to access it. And in fact, if information is encrypted,
you’re also protected a bit from possible penalties in litigation that might follow. So it became important to us that we use this three-pronged approach in all aspects of protecting our assets.

[MUSIC PLAYING]

Interoperability, Standards, and Security

Additional Content Attribution

Creative Support Services
Los Angeles, CA

Dimension Sound Effects Library
Newnan, GA

Narrator Tracks Music Library
Stevens Point, WI

Signature Music, Inc
Chesterton, IN

Studio Cutz Music Library
Carrollton, TX