Considering Security and Privacy in the Move to Electronic Health Records
Transcript

Part 1: Benefits of Electronic Health Records

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a principal researcher at CERT, working on operational resilience and software assurance.

Today I'm very pleased to welcome Deborah Lafky. Deborah is with the U.S. Department of Health and Human Services. And I'd also like to welcome back one of my colleagues, Matt Butkovic, who is CERT's team lead for the work we do with Deborah's organization, which we'll be talking about in today's conversation.

So today the three of us will be discussing some of the security opportunities and also some of the challenges that healthcare providers face as they move to electronic health records. We'll also be discussing two initiatives that Deborah's very familiar with and engaged in that are facilitating adoption of health IT in the United States, and these will be the Health Information Technology for Economic and Clinical Health Act, referred to as HITECH, and also Deborah's office, the Office of the National Coordinator for Health Information Technology, ONC.

So with no further ado, Deborah thank you so much for making the time to speak with us today.

Deborah Lafky: Thanks very much Julia. I'm very pleased to be here and share this time with you and Matt.

Julia Allen: Great. And welcome back, Matt; good to have you back on the podcast series.

Matt Butkovic: Good to be back, Julia.

Julia Allen: So Deborah, to set the stage for our listeners who are not actively involved or not very familiar with this whole national move to electronic health records -- we sometimes refer to them as EHRs, -- could you please summarize what the objectives are of this very important national effort?

Deborah Lafky: Sure. Thanks, Julia. I'll start by saying that it's difficult to sum it all up in a brief statement. It's a huge effort, it's a multi-year effort, but one that we all feel very committed to as the way forward to a significant improvement in healthcare for individuals in the United States. The HITECH Act was passed by Congress as part of the stimulus bill at the very beginning of the current Administration.

And it has a number of objectives that revolve around adopting electronic health records. But it's more than just adopting them. It's all about adopting them in a way that will benefit people, and not just for the sake of having electronic health records and having computers in doctors' offices, if you will; and that's the concept of meaningful use.

We need to have physicians and patients share in their care for the share of information, and use these records in a meaningful way to improve their care. This is an extension of efforts that have been going on for actually quite some time. The federal government started studying the feasibility

of electronic health records back in the early 1970s, when I was still a student at Carnegie Mellon; and it's been going on ever since.

Deborah Lafky: With the HITECH Act, there has been significant funding to help us pursue this goal that we've had for quite a long time, to bring the benefits of automation to the healthcare arena where they've really not been adopted except by very small numbers of physicians and hospitals.

We've seen through some bright spots on the horizon that care really can be improved with electronic health Records. And I will give a little example of that in a minute, related to our beacon communities. But some of the things that we're trying to do are provide some key benefits for providers and patients -- providers being physicians and nurses and all others who are involved in care.

We want to make sure that people have complete and accurate information about their care. Because that's the key to avoiding medical errors, which has been one of the real drivers for wanting to adopt electronic health records, is to avoid errors -- avoid duplicate prescriptions and duplicate tests and mistaken prescriptions and mistaken diagnoses; avoid getting patients confused with one another. These are the kinds of errors that were identified by the Institute of Medicine as being a real source of concern with the healthcare system as it has existed up to this point. And it's widely perceived that electronic health records will go a long way toward helping us resolve some of these errors.

It also helps to give better access to care. It means that doctors can share health records with one another when they share the care of a patient. So your primary care physician can easily transfer your electronic health record to a specialist, or more than one specialist if you have a complicated case. They can ship them electronically rather than perhaps faxing them or having you hand carry them from one place to another. And they can be assured of being more accurate if you do it this way. So information sharing is a really very important component of this.

Julia Allen: May I ask you a question about that?

Deborah Lafky: Sure.

Julia Allen: So then would you anticipate -- because I know, based on the little bit of research I've done -- would you anticipate then that healthcare providers that support a particular patient would then be able to do things like share test results, so that we wouldn't have to have so many duplicative tests done for a patient? Might that be one of the outcomes?

Deborah Lafky: Absolutely. And one of the really important things that they'll be able to do is to move those lab results directly from the lab to any provider who needs to have access to them electronically.

Julia Allen: Great.

Deborah Lafky: So you don't have to get the results from your doctor and then take them to another doctor. That other doctor can get them straight from the lab.

Julia Allen: Excellent.

Deborah Lafky: It makes it much simpler.

Julia Allen: Anything else you wanted to say about benefits?

Deborah Lafky: I wanted to talk a little bit about how important this is for us as individual patients. Being able to potentially access your records electronically right at your desktop means that it's easier for you to manage your own care and to really understand what's going on with it. As well as if you're responsible for other family members -- like a lot of moms are, like me -- you have to manage your children's healthcare records oftentimes. And it's much easier if you can have this all pulled together on your desktop and be able to access it when you need to access it and not have to try to find it in paper records.

Julia Allen: So the intent would be for providers as well as patients to have access to their full medical history, correct?

Deborah Lafky: That's right.

Julia Allen: Okay. Were there some other things that you wanted to say about the transition from paper to electronic records, in terms of services or benefits that might derive, or have we pretty much covered that?

Deborah Lafky: Well I think there's really more to that story. People are very used to paper records. People have been comfortable with those for a very long time, and it can be a little daunting to think about changing all of that over to electronic records.

But when you think about some of the things that electronic records can do, or enable you to do that paper records can't, you have to ask yourself why have we waited this long? If you are (this is the classic case) if you're taken to an emergency room and you can't access your paper records -- say your primary care physician's office is closed -- it's much easier if you have an electronic record that the emergency room can access, for them to fully understand everything that's going on with you so that mistakes can be avoided.

For example, if you're a diabetic, they may be able to see that you, or diagnose that you are in a diabetic crisis rather than trying to figure out a number of other reasons why you might be less than fully conscious.

So that's the kind of care that can be enabled with electronic records, that you just don't get with paper records. Nobody carries around their medical records in paper form, just on the off chance that they would go to the emergency room.

Part 2: EHR Security and Privacy; Regional Extension Centers and Beacon Communities

Julia Allen: Right, right. Well, I'm sure we could spend a whole podcast just on this particular aspect of it. But I would like to move us along. And as I listen to you speak, one of the things that occurs to me -- and I'm sure to everyone because we're all patients in some aspects of or times in our life -- is the security and privacy of all of this very, very sensitive information.

So could you summarize from your office's point of view what some of the key security and privacy requirements are that providers need to both address and satisfy when they're doing this migration from paper to electronic records?

Deborah Lafky: Sure, I'd be happy to. And that's really the sweet spot for me because that's the area that I specialize in within the office where I work.

A couple of things to remember. The Department of Health and Human Services is responsible for the privacy and security of medical records and regulating that and writing the rules surrounding that. And most people are probably familiar with the acronym HIPAA, which is the rule that governs

privacy and security for health records. And it's the rule that's responsible for you having to sign a form perhaps every time you go into the doctor's office stating that you've read their privacy policy.

It's really been key in helping people to understand that they do have this attention to privacy for your healthcare records and that they just can't be used as if they were public information. It's private, it's sensitive, and so it's very important that they be secure. Because if you don't keep them secure, then they're not going to be private.

Deborah Lafky: The HIPAA regulations cover both privacy and security, and they have specific instructions for people who handle medical records -- especially physicians and clinics and hospitals who are called what we call *covered entities* -- specific rules about things that they have to do to keep your medical records secure, and about who can see them and who can't see them, and for what purposes they can be used. And it's all spelled out in that regulation. And that applies to paper records and electronic records.

So even though we're moving from paper records to electronic records, the rules still apply. You still can't just let people see other people's medical records without a good reason. And one of the things that the program I work with -- which is on security for medical records, for electronic medical records -- is to see what additional tools we can develop that will help providers keep these records secure.

And that's actually what we're working on with Carnegie Mellon, is one of these tools that will build up a good basis of security that providers can rely on and make sure that they are following the requirements for keeping these records private and secure.

Julia Allen: Excellent, excellent. If I may, I'd like to bring Matt into the conversation. So Matt, obviously at CERT we do lots of work in protecting and sustaining critical and sensitive information. So from your point of view, what do you see as some of the key security requirements that we need to apply to this sensitive data?

Matt Butkovic: Julia, I think that we have to focus on the fundamentals, to understand that at the end of the day we're protecting a critical asset in the form of patient information, an asset that's critical at the personal level for the patient, critical for healthcare organizations, and also critical at the national level. So I'd say that the goal is to ensure that we've got justified confidence in the confidentiality, the integrity, and the availability of medical records.

Organizations that are moving from paper records to electronic records need to keep their eyes on the fundamentals. The things that they did to ensure the safety and soundness of those paper records also apply in the digital setting, with a few additions.

We need to ensure that the risk management profile of the organization accounts for this transition to electronic records; that your control environment is adequate to ensure that the new challenges introduced by this electronic medium and this path are accounted for.

Julia Allen: So you've got these security requirements. They're fundamental around the whole arena of IT and information security that we've been addressing for a very long time applied to this specific domain.

So what do you see, based on your work, as some of the practices -- security and privacy management practices -- that we actually are working with Deborah's organization to recommend to help ensure that these records are secure in electronic form?

Matt Butkovic: Sure. I think the theme here again is focusing on the fundamentals. And one of the things we've done with Deborah is develop a tool that helps identify the absence or the presence of key management practices required for the appropriate management of EHR.

I would say that identifying and understanding the linkage between your assets and the critical services -- in this case healthcare -- you deliver is one of the key insights. So we're hoping to -- and I think that the program has been very successful in creating the products that will equip folks in the healthcare community practice to identify those critical assets and also identify the safeguards and the condition of the safeguards that surround those assets.

Julia Allen: Would it be fair to put you on the spot to give us an example or two of a critical service, and maybe some asset-level practices to ensure that service is performed securely?

Matt Butkovic: Sure, not a problem. Let's stay grounded with something very practical and let's look at incident management. One of the things we'd advocate, based on our years of experience in incident management and also as articulated in the CERT Resilience Management Model, is that you must have a mechanism to identify and respond to an incident.

Now that could take many forms. In the paper record world, you had a way to understand the disposition of your records. Paper records, by definition, were tangible and if they walked out the door, they walked out the door in dribs and drabs, not in kilobytes of information, as we have today.

So we would say that one of the key practices that everyone must maintain to adequately manage electronic records is the ability to identify that there's been some alteration or exfiltration; that is, records leaving an organization. And that can take many forms. That can be a network intrusion that results in information being removed from your organization. Or it can be as simple as someone taking a USB drive home that's unencrypted, which is unfortunately a recurring real-life example of a lapse in the control environment that results in the breach of medical records.

Julia Allen: Excellent. Thank you for those examples. So Deborah, just as we're moving in this direction, I'd appreciate an opportunity for you to tell our listeners a little bit about the role of your office, and how you're specifically working to facilitate adoption of electronic health records. Could you say a little bit about that?

Deborah Lafky: I'd love to, and thank you, Julia. Our office was established actually in 2005. It's a very tiny office within Health and Human Services. And we've established a beach-head of working on having providers adopt electronic health records because we understood the value of it, and we were trying to encourage this to happen through various channels.

With the HITECH Act, we, our office, was funded with a fairly large stimulus package to really push this forward. So our office is called the Office of the National Coordinator for Health IT, which is pretty self-explanatory.

We report directly to the Secretary of Health and Human Services. And our real goal is to foster the adoption of electronic medical records by the end- users, the providers -- so the physicians, the clinics, the hospitals. It is not focused on developing some national system of medical records; that's not what this is about. But it's about getting every doctor's office to have a modern information system that deals with people's health.

And so we have several programs that we are running right now, thanks to the stimulus package that we received, including our Regional Extension Centers, which are much like the Agricultural Regional Extension Centers -- the farm bureaus that you write to and you find out how to grow crops better.

We've implemented that same idea for providers, with 62 Regional Extension Centers throughout the country, where providers can go and get the help that they need. Because most of the primary care in the United States is delivered by medical practices of one to five doctors; small offices. They don't have IT staffs. They don't know how to set up a computer network. And so we've put the resources out there, with this funding, to help them.

And one of the other programs that we have that is helpful in this area are called *beacon communities*. These are highly focused practice clusters, if you will, in communities that involve hospitals and practitioners and clinics working together on a specific problem and using electronic medical records to help, for instance, reduce the incidence of rehospitalization after discharge, or reduce the incidence of admissions for diabetes.

Deborah Lafky: We have these beacon communities that are figuring out what the best practices are, so that we can then take those and show the smaller providers that aren't connected to the beacon communities how to use them; how to use these practices to really improve people's health.

So in the end, although our goal at the ONC as we're known, is to foster the adoption of electronic health records, the real end-goal that we're all working toward is to improve healthcare and the quality of care and reduce the cost of care throughout the whole country.

Julia Allen: So would it be fair to say -- as I think about operationalizing what you're talking about -- would one example of how your office works would be in the process of both setting up and working with these regional centers and these beacon communities, taking some of the best practices out of the beacon communities and packaging them or documenting them in a way that they're available to the regional centers? Would that be a fair characterization?

Deborah Lafky: Absolutely, and in addition to documenting and disseminating those best practices from the beacon communities, we are collecting input and sponsoring projects (such as the one that we're doing with Matt's group right now) to foster best practices in other areas where the beacon communities are not active. And privacy and security is one of the major areas that ONC has taken the initiative to create, document, and disseminate these best practices and get people trained on how to use them.

So one of the things that Matt's group is doing for us is to implement the training program for incident response that providers will be able to come to online interactively and learn what this means and how to do it; so how to detect an intrusion, as he just alluded to.

Julia Allen: Fantastic; I appreciate that example.

Part 3: Patients Should Be Ambulatory, Not Their Records

Julia Allen: So Matt, this is a pretty daunting undertaking, and it's got many, many moving parts, and lots of stakeholders, lots of folks who are committed to making this all move forward in a coordinated way. But let's get back to, as Deborah said, to the one to five person office of a provider.

And if I'm a provider and I'm thinking about all of this that I have to do -- but particularly with respect to security, which is often a new thought for folks that work in a very small local community -- what might be some of the first steps that I would want to consider to make sure that my patient data in electronic form is secure?

Matt Butkovic: Sure Julia. I think I'd like to start that answer by saying that it *is* daunting. But we should remember that it can be decomposed into digestible chunks. As Deborah's describing,

there's assistance provided by ONC and there's very specific things we can do to aid that process of ensuring that your EHR is secure.

Understanding how this fits in your overall risk management process I think is the key. So whether you're a small provider or a very large provider, you're managing risk; you're managing risk in many forms. And this is another flavor or another thread or stream of risk that you need to manage.

So I think understanding -- just to reinforce the point about assets -- understanding the connection between delivery of your critical service's assets, and then your risk appetite, and the safeguards around those assets is really the key. So it sounds very hypothetical. But we're equipping providers to evaluate their current posture and make improvements based on that analysis.

Julia Allen: So can you give -- again, I'm always pressing you for examples, just to make the concept a little more clear. So can you think of an example of a risk that a smaller provider might face, and how they would factor in ways to mitigate or manage that risk as a step towards this initiative?

Matt Butkovic: Sure. Let's continue with the example that I mentioned earlier of the unencrypted USB drive, which is sort of a headline grabbing, very real-life example. If you have electronic medical records and you allow portable storage, like thumb drives or USB drives, you'd want to understand how those are being used, and understand if medical records are making their way to those devices. And at a minimum ensure that you have provided a safeguard in the form of encryption so that if that device does leave your hospital, that the information is protected.

That's a very basic example and there are many nuances in there we didn't explore. But to give you a real- world, tangible example, ensuring that medical records don't walk out your door on portable electronic storage would be one of those things I'd point to as a quick win; understanding the disposition of your records, where they reside, and ensuring you've got safeguards to prevent the mass exodus of information from your hospital.

Julia Allen: Great, great, that's really helpful. Did you want to add something to that, Deborah?

Deborah Lafky: One of the things that I try to keep uppermost in my mind when I think about this is that it should be the patients that are ambulatory and not their records.

Julia Allen: Oh that's a good tagline. I like that.

Deborah Lafky: But just to add to what Matt said, you have to think about your risk profile. And if you put it in very concrete terms, often it's easier to think about it.

So there was a recent incident last month of a hospital somewhere on the East Coast that had an unencrypted hard drive stolen out of an employee's car. It had 88,000 medical records on it. And I did a little bit of a calculation to find out if those were paper records what would that mean for that particular practice, and found out that if you took all of those medical records (if they had been in paper form) and stacked them up, they would be taller than the tallest building in the world.

Julia Allen: My goodness.

Deborah Lafky: And when you start to put things in concrete terms like that, it's a little bit easier to understand your risk and try to take the right steps to mitigate it.

Julia Allen: Excellent, excellent example. So Deborah, do you have some favorite places that you like to refer people, where they can learn more and delve more deeply into this subject?

Deborah Lafky: Well, it's a deep subject to delve into. But we can start with the newly launched ONC website. It's called healthit.gov. And our old website, which also has a lot of our detailed technical information on it, is confusingly named healthit.hhs.gov. But both of those are live and active websites: healthit.gov and healthit.hhs.gov. And in addition, there's good technical information available through any of the Regional Extension Centers.

For those who don't know where their Regional Extension Center is, they can find out at our website, healthit.gov. And there are technical papers and publications available through our website and also through the National Institute for Standards and Technology (NIST) who've done several excellent publications on risk management, risk assessment, and risk assessment in the context of health IT.

Julia Allen: And you had mentioned training opportunities. So if folks kept tabs on new content posted to your website, do you anticipate either making that notification of training or even the training materials available via your portal?

Deborah Lafky: I'm glad you asked because we have an extensive set of training modules that we're going to be launching over the next nine months. And our first one, which is going to be health IT security 101 -- it's very basic -- will be accessible to everyone; very quick and easy to get through. And we hope it will be fun; we're aiming for it to be fun. And that is due to come out right around the end of this calendar year.

Julia Allen: Excellent. And Matt, do you have additional sources that you would like to add to the ones that Deborah has discussed?

Matt Butkovic: Sure, Julia. I think that cert.org, if you go the spaces dedicated to resilience management and incident management, there are many publications and lots of great material that's publicly available that speaks to the concepts that we've discussed today.

Julia Allen: Excellent. Well, Deborah, I cannot thank you enough, as I said at the top of our conversation, for making very precious and valuable time available to help us reach out to our listeners on this important national initiative. So thank you so much for your time and expertise.

Deborah Lafky: Thank you, Julia. I'm delighted to help.

Julia Allen: And Matt, great to have you back on the series. And I'm sure I'll be hitting you up again. But appreciate the fine work you're doing with Deborah's organization and talking about it today.

Matt Butkovic: Thank you, Julia.