Electronic Health Records: Challenges for Patient Privacy & Security
Transcript

Part 1: Technical, Social, and Political Hurdles

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 Melon 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 senior researcher at CERT, working on operational resilience and software assurance. Today I'm pleased to welcome back Bob Charette, founder of ITABHI Corporation. Bob is also an internationally recognized expert in risk management, information systems and technology, and systems engineering. Today, Bob and I will be kicking around what's happening with electronic health records, including progress to date and specifically the challenges for security and privacy. So welcome back, Bob. I'm really glad you could join us today.

Bob Charette: Well thank you for inviting me again, Julia.

Julia Allen: Okay, so for our listeners who aren't real familiar with the current status of electronic health records - and I know we've been hearing quite a bit about these, with respect to the current administration's health care agenda in the United States - could you just start us off with a little overview?

Bob Charette: Sure. Well let's go back a few years. The whole push for electronic health records in the United States is from a governmental policy, although it extends probably all the way back into the 1960s if you were to draw a history. But if you go back to President George Bush's State of the Union Address in 2004, he called for all Americans to have an electronic health record by the year 2014.

Now, an electronic health record, although there's lots of different definitions - some of them are called electronic medical records, personal health records, etc. Basically you can think about all of your medical records being digitized. And that includes your records from your eye doctor, from your dentist, from your physician, from the hospital – anybody who's a health care specialist in the broadest sense - that all that information that exists in a paper record would be digitized.

And that information would flow across what is generally called a National Health Information Network, which might be the internet. It may be a specialized network. People are still arguing about exactly what that looks like. And that information would be available to any health care provider anywhere in the United States with almost instant access.

Julia Allen: So would this include my having the ability to access it myself, or would it only be my doctors?

Bob Charette: Well that's a good question. The idea is that you would be able to access that electronic health record yourself and you'd be able to make sure that there weren't any mistakes on it. You would also be able to define who would get access to it, who would have the access rights and so on. That's the concept anyway.

There's also, there's been discussions about, well, should that information be readily available to everyone unless the patient puts access controls on those? So as you start to actually define what you can and can't do with electronic health records, the technical issues become, and as also social and privacy issues become, very complicated very quickly.

Julia Allen: Well let's talk about that. Because just based on the little description that you've provided us, this seems like a no-brainer to me. I mean, it would be great to be able to not have to take the same tests over again, have all of my conditions, under my auspices, be available to my health care providers. And certainly with the explosion of the internet for use in all aspects of business, this really does seem like a natural application.

But you did start to talk about - I'm sure there are some pretty significant technical, social, political issues. A little bit later, we'll be talking about security and privacy but what kinds of issues make this such a daunting undertaking?

Bob Charette: Well let's start a little bit with just the technical issues. Let's take one of the, just one topic in particular. Let's talk about interoperability where all your information that is generated on you is able to be communicated to others in a form that's readable. Right now there aren't any set standards for how information can be defined and made interoperable. There is a doctor who, when I interviewed him for a story I did for IEEE Spectrum a few years ago on electronic health records, said, "Well, one of the problems is basic communication. There's 160 or 170 different ways to describe high blood pressure." So there isn't - even the basic terminology in medicine isn't well defined and accepted.

So we have communication issues both in terms of language and in terms of just standards in media - trying to make sure that we could standardize how information is captured and then communicated across a network. And within a hospital, most people don't understand that a typical hospital has 270 different IT systems that are operating at one time. And these systems include everything from CAT scans to x-ray systems, to your blood pressure system, and all these are capturing information. All that information that's being generated has to be able to be captured in some way into an electronic medical record and stored and transmitted.

There's a tremendous amount of disagreement, in fact, in how much information should be captured, and transmitted at any particular point in time. There's

argument that says that all your patient information should be captured in one place, or captured electronically, but only summary records, a small portion of that record ought to be communicated across the network. Then you also have the issue of billing and administration. So all these systems not only have to interact from a medical perspective but they also have to interact in terms of how do I get paid, how is that billed? And then that information has to be sent to insurers who also have to be able to interpret that information.

And so just from a - as you start to draw a simple flow chart of how a piece of digital information flows through a network, goes out and then is captured. And, by the way, is going to be stored for a person's life, right? Somebody - this isn't just going to be there and then disappear. This is my children who are young, when a network comes into play, or an electronic health record comes into play. For the next 80 or 90 years, that information is going to be added to and have to be kept and updated, etc.

So all these little issues, none of which individually seem to be that difficult, cascade very quickly. Then when we add in, from a doctor's perspective, we have workflow issues - working with computers versus working with paper records - require you to think differently in terms of how you're going to actually make use of those systems. There's been lots of complaints by patients, when doctors go to electronic health records, that the doctors are more interested in communicating with the computer than they are communicating with the patient.

So it becomes a very large set of problems. And we haven't even touched on - let me talk about the political for just a moment. From a political standpoint, the real underlying push is for reduction of cost. The patients, the savings are very, very important. And in fact the previous [U.S.] administration talked about electronic health records being a way of saving Medicare by being able to reduce the cost of Medicare.

Now you can increase patient quality and reduce cost. But the organizations that have been able to do that - like Cleveland Hospitals and Cleveland Clinic and the Mayo Clinic - they've spent well over a decade working out how to make those electronic health records work and improve the quality of care. So it's, from a technological, social, political issue, it's probably the most complicated area of IT that exists today. It's much more difficult than defense.

Julia Allen: That does tend to make it a pretty challenging issue and it touches every single citizen. So everyone has got needs and opinions and requirements and views on the matter, I suspect.

Bob Charette: And I think that's an important point. Every person is going to be affected by electronic health records. And so everyone has a stake in how these things are developed and how they're paid for. These things aren't going to be free. The current administration, in part of the American Recovery and Reinvestment Act, set aside $19.2 billion as incentives for hospitals and physicians to invest in electronic medical records, assuming that a. they met standards and

b. there was something that's called, "meaningful use," which says that the doctors actually use these things rather than just make the investment.

But at the same time, the administration is also setting up other types of incentives and disincentives in terms of payments for government health care - that if you don't use electronic health records, for instance, in certain situations, doctors will find that their reimbursements are cut or otherwise, they'll be also increased if they do use them. So this is going to affect basically one fifth to one sixth of the total US economy, which is much greater than defense.

Part 2: Privacy: Disconnects between Law and Reality

Julia Allen: Absolutely. Boy, you raised lots of interesting and challenging issues that I would love to pursue but let's stay on point here and turn our attention a little bit to privacy and security. So clearly privacy is a huge issue and we've talked about how this affects every single individual. When it comes to specifically patient privacy or the privacy of my electronic health records, what do you see as some of the key challenges, and perhaps even some potential solutions?

Bob Charette: Well the key challenge, really in terms of privacy gets back to something that we have touched on before, which is who gets to see this? Part of the - the number of doctors I interviewed, especially those who were treating patients with mental illness, they're worried that if the information, the personal information of their patients, leaks or has the potential for being leaked then those patients won't come in for treatment.

And we've seen cases where famous folks have had their medical records looked at by lots of different folks and also been spread out to the press. Hospitals in California have been fined several times for not having really good privacy controls on movie actresses and, for instance, the octuplet mother had some of her records looked at. Michael Jackson's death records have been leaked to the press and the sheriff is involved in trying to find out how that happened.

So the argument has always been that electronic health records are more secure than paper records, which is probably true in one sense. But at the same time, the likelihood of lots of records being exposed by hacking is much greater than before. Here in Virginia, for instance a hacker got into the Virginia system for prescription drugs and basically has held millions of patient records for ransom.

So this whole area of privacy - and again it touches into security; you can't really separate the two - has become a very big deal. In fact, the privacy-security area is called the third rail of electronic health records. People are working very hard at trying to address this. People are looking at biometrics, they're looking at secure credentials, they're looking at just about everything in the book in terms of how to make this - make privacy a very key element.

But one of the problems I've seen, and again it came out very clearly in my research, is that privacy has not really been a (and the same thing with IT security

in the electronic health record area), hasn't been built in as a fundamental notion. A lot of it is addressed by policy or administrative law, which again doesn't really affect very much in terms of system design. So this is going to be something that I think that is going to be the biggest hurdle for getting people to accept electronic health records.

Julia Allen: I know in some of your writing that you've done, some of the issues that I hadn't thought about before is, you talk about if you're staying in the hospital, all the different people - nurses, x-ray technicians, billing clerks, other administrative staff - the access control and identity management issues around electronic health records are substantial. When I think about the equivalent today, everybody has access to your paper file as well so maybe that's not that big of a consideration. You think all the different people who might have access or be able to take a peek?

Bob Charette: Well I think the problem is that, although paper records people can, again, the same number can get at them. I think what happens is that when you have electronic health records, unless you have very strong credentialing, the number of inputs into the system is much greater. A paper record, somebody has to go in and get that physical access to it.

Julia Allen: Right, it's much more local.

Bob Charette: It's much more local. And so you – so electronic health records, the likelihood is much lower but the consequences can be much higher because you can spread them across the net very quickly. If you take a look at what happens at Mayo, the Mayo doctors and the folks who can look at a record, everyone has a card and has a particular identifier, and they know every single person who has looked at a record. No record can be looked at without it being matched against a credential.

Now that being said - and I haven't heard it at Mayo but I've heard it in the UK where they have used some of these systems, where people have borrowed somebody else's card to get into the system. So no system is foolproof. And I think what you have to do is, you have to have some type of combination of credentialing as well as patient control so that you can try to limit that. But even again, like going to a hospital, I don't think a patient is going to be able to determine which one of those 150 people who get to look at their records, gets to and who doesn't.

Julia Allen: Right, that has to be built into the system.

Bob Charette: It has to be built into the system. So it gets - this is why it becomes very, very tricky. We're not talking like a Visa system, a transaction processing system, where we're talking about a single piece of information. We're talking about lots of different information flowing in from lots of different places that are now being combined and also being split back up to move to a lot of different locations. So it's a difficult problem.

Part 3: Security: Patient as Advocate

Julia Allen: So what about information security? I know we tend to conjoin security and privacy quite a bit. But with respect to information security, are there aspects of protecting electronic health records specifically where the standard information security controls that we use for protecting any sensitive information? Do those apply, are there other ones, are there differences that you've run across that we need to take into account?

Bob Charette: I don't think that there's really differences or anything that's specific to electronic health records per se. As I mentioned earlier, the real differences have been more in terms of reporting breaches and who is responsible for protecting that information. We've had a HIPAA law, Health Insurance Portability and Accountability Act, since 1996, which sets out what covered providers need to, or covered entities need to, do in terms of protecting patient privacy. And that's been upgraded this past year, called the HITECH Act, which is the Health Information Technology for Economic and Clinical Health if I've got that correct - which again points out that any entity that holds or transmits health information needs to tell folks when that information has been breached.

But again, it's been more in terms of the law rather than in terms of any type of pure technological approach. And I think this is has been one of the issues in terms of, you may have this law but how well is it really enforced? The HIPAA law for instance, has only been enforced to its fullest extent maybe half a dozen times in the past 12 years. So you have people like Google and Microsoft who claim that they're not covered while the Federal Trade Commission says that they are covered by these Acts.

So again it's really more of a kind of closing the barn door after the horses have escaped. And so I'm not sure if I'm really answering your question very well but all the technological approaches that you see normally are in use. It's just more in terms of what happens when a breach occurs that is more universal than the normal information security area.

Julia Allen: Well it seems to me that when we look at things like security risk assessments or other types of processes for going in and assessing the security state of a system, that maybe perhaps we'll see more rigor in or a higher threshold of controls that you need to demonstrate satisfaction of, for a security risk assessment that's conducted against the system that holds electronic health records. I don't know if that's a potential ...

Bob Charette: That's a potential but to be honest, I think what one of the problems is that we have 112,000 or thereabouts private practices in the United States. And we're expecting that those 112,000 - and that doesn't count optometrists and all those other thousands of other offices that electronic health records will eventually touch on - is that we're expecting all these small organizations to be security aware and to do those types of risk assessments and

to look at those types of things. And I think this is again where there's a disconnect between what we put into the law and what we expect people to actually do. The small practices, we're going to ask them to be small IT and high security shops and I think that's going to, that's asking a lot.

Julia Allen: Well it also occurs to me that there's a business opportunity here for those who want to get into the business of helping small medical practices. But I'm also reminded of patients and each of us as individuals having to become our own advocates when it comes to our own health care. And I'm getting this uneasy feeling that we're also going to have to become our own advocates when it comes to the security and privacy of our electronic health records, which seems a little unfair.

Bob Charette: Well I think you're absolutely right though. I think that individuals will have to be much smarter and more aware of how their records are being used and the level of security that the local, your local physician actually has in those.

Julia Allen: Well, I think of consumer watch groups and things like that. I mean this is clearly going to be a problem space that's going to evolve over the next several decades and I think there are lots of opportunities to try and help move this along. But it seems like progress is going to have to be very deliberate and carefully considered.

Bob Charette: Well I fully agree. Again, my biggest concern has been that across the board, when I wrote my article back in 2006, we were - the industry and the government were - had a number of fundamental issues that had not been fully addressed or fully understood. And here we are in 2009 moving full speed ahead without having answered almost any of those questions.

And so again, I'm a little uneasy about how everything is going to work and how privacy and security are going to work as we rocket down toward this goal of having electronic medical records for every American, probably not by 2014, but the current goal is definitely by 2020. So without really understanding all the implications, it could get to be a little messy along the way.

Julia Allen: Well, Bob, I mean this is just a great introduction to a very, very complex subject. Do you have some places that you recommend where our listeners can learn more? We'll certainly include a link to your work and your articles. But are there some other places you would recommend?

Bob Charette: Well I think, again, if people really want to get up to speed on this, I think that probably going to the Health and Human Services site for the government, Health Information Technology site, is one area that they really need to take a look at. There's a great magazine, Government Health IT, that's out there that covers this in great detail. There's Modern Health Care, which is another magazine that's covering this. There are some books out there I like, Michael Porter's book on Strategy For Health Care Reform because if you're going to have health care reform, you're going to have to also reform the whole area of IT and

health care. And it's – the biggest issue here is that the target is moving very, very rapidly, so you can get a snapshot but six months from now it probably will change radically because we're building it.

Julia Allen: Well Bob, thank you so much for your time, expertise, for shining the light on this tough issue, and we'll keep an eye on this space.

Bob Charette: Thank you very much.