

Security Questions to Ask EHR Vendors

Interview with Eric Nelson, privacy practice leader at the Lyndon Group



July 13, 2010 – Howard Anderson, Managing Editor, HealthcareInfoSecurity.com

Physician group practices should ask electronic health records vendors tough questions about privacy and security before selecting a system, says security specialist Eric Nelson.

In an exclusive interview, Nelson, privacy practice leader at the Lyndon Group, Newport Beach, Calif., says practices should:

- Make sure the EHR vendor they select is willing to sign a comprehensive business associate agreement;
- Confirm the EHR vendor is willing to be audited for compliance with HIPAA privacy and security rules; and
- Determine whether an EHR vendor that remotely hosts an application via cloud computing is willing to spell out how the practice can retrieve its clinical information if the company goes out of business.

Nelson also advises practices to:

- Develop risk assessments addressing six key components before installing an EHR;
- Take steps to guard against improper disposal of paper records when making the shift to electronic records; and
- Make extensive use of encryption.

As practice leader at the Lyndon Group, Nelson helps healthcare and financial services clients address privacy and information security issues. He is a Certified Information Privacy Professional and specializes in federal, state and international privacy and information security compliance and breach mitigation. Nelson is a member of The Privacy Consortium, a collaborative group of privacy experts.

HOWARD ANDERSON: This is Howard Anderson, managing editor at Information Security Media Group. Today we're talking with Eric Nelson, privacy practice leader at the Lyndon Group. Thanks so much for joining us today, Eric.

ERIC NELSON: I'm glad to be here.

ANDERSON: Across the country, many small physician group practices are planning to acquire their first electronic health records system and hoping to receive federal incentive payments under the HITECH Act. So what questions should group practices ask electronic health records vendors about privacy and security when they're

shopping for a system? And should those questions vary depending on whether or not the system works using cloud computing?

NELSON: Under the new HITECH Act, anybody who is sharing information or collecting information or managing information for a practice...is now considered a business associate that also has to meet HIPAA security and privacy requirements....So is the vendor willing to sign a business associate agreement, and what are the contractual assurances? For instance, are they willing to be audited...to make sure that they're continually compliant with HIPAA privacy and security regulations?

Another question is what kinds of administrative, technical and physical safeguards are in place with the vendor, and what kinds of procedures and tools are in place to restrict and monitor access to a practice's confidential information? And finally, if the EHR is administered by a third party, and it doesn't matter if a practice hosts the system onsite or whether it's hosted via the cloud, will they provide specific information on the hiring and oversight of administrators, technicians and controls over their access to your information?

Now, specifically with the hosted or cloud environment, some of the key questions to ask might be: How is that data secured, and is the facility where it's hosted certified? Can the vendor provide detailed information on its security architecture? And are they willing to accept a security audit if a breach occurs? Or if their building gets blown down, what are the response procedures that are in place?

And finally, and this is an area that a lot of people might not even think about, but how would you obtain and protect your information if a vendor fails or is acquired by another company? Those are the key questions I would ask.

ANDERSON: So how can a smaller group practice with relatively limited resources conduct a meaningful risk assessment? Should that be done before the EHR is installed?

NELSON: Well, a risk assessment should be completed definitely before a system is installed. The HIPAA security requirements protect the confidentiality, integrity and availability of electronic protected health information. The HIPAA security rule actually requires the covered entity to perform a risk assessment that identifies reasonably anticipated threats, hazards and unauthorized use and/or disclosure....

Every practice has to make a conscious and legitimate effort to meet the HIPAA security requirements. Now, regarding a risk assessment and the questions you should consider, there are six main components:

Does the practice have general security standards and policies in place?

Does the practice have and maintain appropriate administrative policies and procedures related to its workforce?

Has the practice identified and addressed potential risks as it relates to the physical environment of its data?

Are appropriate technical controls in place to protect electronic health information and restrict unauthorized access?

Does the practice have appropriate agreements in place with business associates that they share health information with?

Now, one of the things that a practice needs to understand or consider is that they're not just protecting patient information, but they also have employees, and they also have contractors that work for them. So some of the information that they may be collecting and sharing may not be protected health information but they may be sharing it with others, perhaps outsourcing some of their other functions. This includes, for instance, payroll, benefits or other processes within the organization.

And then finally, does the practice have written policies and procedures that comply with the security rule?....And do they keep their information updated specific to that documentation?

Those are the six primary components of the security rule. But the HITECH Act, coming into play last year, had additional privacy considerations. Probably the most significant...is breach notification.

Outside of the HIPAA and the HITECH requirements, one of the most important steps before implementing any type of system is an inventory of the personal information that a practice collects, manages and shares.

The reason for an inventory boils down to, "How can you protect something when you don't know what you have to protect?" So a small practice, a medium-sized practice or even a large organization should understand what information they have, down to a data element level, meaning a name, an address, a driver's license number. I'd include Social Security number, but that's one thing that a lot of practices shouldn't collect, but they often do.

Practices need to understand exactly what individual data elements they're collecting, how that information is being collected and why that information is being collected.

The inventory should also identify who has access to that information, do they need access to that information to perform their job and if they don't, does that information need to be restricted? And finally, the practice should determine how that information is shared and how that information is retained.

Again, it boils down to how can you protect something when you don't know what you have to protect?

ANDERSON: In general, then, what are the main security risks that a practice faces when shifting for the first time from paper-based to electronic records? What are some of the best ways to minimize those risks?

NELSON: The HIPAA security rule applies to electronic protected health information. The privacy rule applies to all protected health information, be it on any type of media it could be electronic, could be paper, could be somebody talking.

Probably the highest security risk is protecting paper records from unauthorized access during and after a transition to an electronic health record system. A couple of examples would be if there's a third party that's coming in to do the transcribing or the conversion, such as by scanning documents, how is that information being managed? And does the third party subcontract out any work? What are their policies and procedures? And what are their safeguards to protect that information?

And the second key area is improper storage or disposal of paper records. Probably a week doesn't go by where there's a news clip out that talks about some kind of company...where somebody discovered an entire trash bin full of personal information. And in fact, I was meeting with...someone who...shared a story about coming upon a medical center about a year ago where some kids had broken into an outside storage locker where the small clinic had just stored their records and the kids had broken the locks off the door and medical records were completely strewn across the parking lot. It was not done maliciously...but somebody easily could have broken in and stolen those records. So improper storage prior to disposal of paper records is one of the biggest threats during the transition to electronic health records.

ANDERSON: Should practices encrypt information, on mobile devices as well as workstations and servers and e-mail?

NELSON: The answer is yes, yes, and yes. One thing that a practice should consider is whether they really have a business need to store information on mobile devices. One of the highest areas of breaches are breaches of a mobile device, primarily laptops. The reason that the information is at risk is because it wasn't encrypted. Now that encryption is starting to become less expensive, it's becoming more prevalent. People are starting to realize how important encryption is, especially on mobile devices. It's imperative to encrypt the information.

In addition, there are at least two states, Massachusetts and Nevada, that require encryption for personal information carried on mobile devices or sent via e-mail. Now, it doesn't include medical information but if there's other information on there, personal information, any kind of financial information, driver's license information, PIN information, that type of thing, it falls under the state notification requirements.

But finally, encrypting information, be it on a mobile device, be it on a workstation or server, can provide a safe harbor against breach notification requirements both for the HITECH Act as well as some state requirements. So encrypting information on a mobile device is absolutely imperative, but it's also good practice to do it on your server and workstations.

E-mail is a little bit different....But...instead of having to go through and download software on a practice's computer and then have the same type of software downloaded on the recipient's computer, there are now hosted services that can provide encryption and do it very easily and do it very inexpensively.

I have one client that uses a particular service that runs about \$65 per license. And if they sent an e-mail to one of their business associates or a patient, all it requires that recipient to do is to enter their e-mail address and enter some kind of a password and they automatically are signed up for that encryption service and they can receive that

information encrypted. So the answer to your question is yes, information should be encrypted....

ANDERSON: Finally, what other security technologies should physician group practices consider?

NELSON: It's not the computers that steal or lose the information, it's the people. And most of your data breaches don't occur from hackers....Especially in healthcare, most of the information is lost, stolen or mishandled or mismanaged because...people either didn't know about the policies, weren't stopped from accessing that information or just didn't know how to handle it properly.

So there are going to be a billion vendors out there telling you what kind of technologies to use. But I think it boils down to the people and the processes and the polices and the procedures, making sure people understand what information you collect, manage and share, understanding who touches it, why do they touch it and understanding how you can protect that information. And if something happens to it, understand how to take the steps to make sure that the damage to both your business and your patients is mitigated and that you retain your good name as a business and practice.

ANDERSON: Well, thanks Eric. We've been talking today with Eric Nelson of the Lyndon Group. This is Howard Anderson. Thanks so much for listening.