Quality Insights Quality Innovation Network
Security Risk Assessments: Meaningful Use and HIPAA Perspectives Webinar
August 26, 2015

Lori: On behalf of the Quality Insights Innovation Team, I welcome you to today's webinar, Security Risk Assessments: Meaningful Use and HIPAA Perspectives. My name is Lori Fink, and I'm the Communications Specialist for the Improving Outcomes by Optimizing Your EHR Initiative. Before getting started, I would like to take a moment to review a few housekeeping items. First, all participants have been muted and will remain in a listen only mode. There will be a question and answer session following the presentation, so if you have a question that comes to mind during the presentation, please feel free to type it into the chat window which can be found on the right of your screen. We will address it during the Q and A session. You're also encouraged to type your questions in the chat box during the Q and A session.

The webinar is being recorded and the recording, as well as the slide deck from today's session, will be posted on the Quality Insights website within the next few days. You will have access to both resources at www.qualityinsights-qin.org under the Events tab as an archived event.

At this time I would like to introduce our first presenter, Adam Kehler. Mr. Kehler is the Health IT Privacy and Security Specialist for Quality Insights of Pennsylvania, which serves as the Regional Extension Center for Pennsylvania East and West. Since January 2011, Mr. Kehler has conducted security risk assessments and HIPAA compliance reviews for over 500 organizations. Mr. Kehler is a recognized leader in the health IT security community and has been invited to speak and participate in various conferences regarding privacy and security. Adam received his Bachelors of Computer Science Degree from the University of Manitoba and holds a CISSP certified ethical hacker, and a certified HIPAA professional certification. He has over 20 years of information technology experience as a network developer, systems administrator, system analyst, IT project manager, and IT security specialist.

Mr. Kehler designed and implemented security systems policies and procedures, and has provided security consulting for many large and small organizations. At time, I will hand things over to Adam.

Adam: Thanks Lori, and thanks everyone for joining us today. I hope you're able to get something valuable out of the presentations. Between Nick and I today, we want to just really address the security risk assessment requirements of Meaningful Use and HIPAA, and talk about what the requirements mean. Later on, Nick will go through the current landscape of audits and expectations of the regulatory organizations.

We are going to start out with a disclaimer. None of this is legal advice, and if you have any particular legal questions, certainly consult an attorney.

I'm going to talk about what Meaningful Use and HIPAA is, dispel some myths that may be out there regarding the security risk assessment, pull out the definitions and

elements of a risk assessment and risk analysis, and give some tips on what you should be doing as an organization in the regard.

Well, that's me. I guess [inaudible 00:04:00] not in person today, you may want to know what I look like. That's me. I work for PA REACH as Lori indicated. She already gave a bit of background, but certainly we've been doing this for a number of years helping organizations meet the Meaningful Use requirements.

Start with the legal and compliance requirements. First a security risk assessment or security risk analysis is of course required by HIPAA and HITECH, as well as Meaningful Use. I know that a lot of organizations I meet with have done a security risk analysis or did not prior to the Meaningful Use program. I know that the financial incentives was certainly a good incentive to do it, but that said, it has been required since the inception of the HIPAA security rule back in 2005 that organizations do a regular security risk analysis. Meaningful use, they really didn't add any requirement to that. They basically just said do your HIPAA risk analysis and make sure to include your [inaudible 00:05:16] EHR.

There are also [inaudible 00:05:19] requirement for security risk analysis. FISMA has requirements in it, certain grants and other accreditation such as ACO have certain requirements for security risk analysis. These often overlap with the HIPAA requirements as well as for Medicare and Medicaid systems, they expect that you're doing a regular security risk analysis. There are a lot of different areas that many of the organizations may be participating in that require this risk analysis.

Meaningful use. First of all, Stage 1 basically, like I said, refer back to the HIPAA requirement. Conduct and review security risk analysis in accordance with the requirements under, and there it refers back to the HIPAA security rule. Of course implement security updates as necessary as part of your risk management process. That requirement is sometimes a little bit vague. It's like, "Okay, how much do I have to mitigate my identified risks?" That's not always a clear answer. [essentially 00:06:26] what I guide practices that I work with in is say, "Okay, have a risk management process. Make sure you have prioritized and addressed the risks that we identified and you certainly have an action plan with target dates that show that you are addressing these risks."

Meaningful use really didn't change much. It's mostly the same requirement, just added the requirement to address [encryption 00:06:52] security data risk as part of the Stage 2 requirement. Now I've always felt that that's an important part of the risk analysis anyways, so I [inaudible 00:07:02] that really changed much, as long as you're doing a good Phase [inaudible 00:07:03] risk analysis. [inaudible 00:07:07] requires that it be stated and revised and updated for each reporting period, so that generally amounts to once a year.

What does [inaudible 00:07:20] have to say about it? Well here's that [HIPAA 00:07:23] rule that Meaningful Use referred to. At the bottom you can see that same number. Conduct an accurate and thorough analysis of the potential risks to confidentiality,

integrity, and availability of EPHI. A few things stick out there. Obviously I've added some bullet points there. Accurate and a thorough analysis as well as confidentiality, integrity, and availability. Often when we think about security, people just think about confidentiality, keeping it private, but you have to remember that it also includes integrity, so how much can we trust the information that is presented us, and availability. We can make something as confidential as possible, but if no one can get to it, it doesn't do a lot of good. We always have to find a balance between those three.

Of course once you have completed risk analysis, take reasonable and appropriate steps to reduce the identified risks to more appropriate levels. Notice it doesn't say completely eliminate risk, because that's generally impossible. They use this reasonable and appropriate standard to determine are you taking appropriate steps to address these risks.

Okay. Myths and facts: these are a few facts. I actually grabbed these from the guidance document on healthit.gov, but there are all things that I've come across out in the field, and so I wanted to spell them out. This is optional for small providers. You don't have to do it if you're a small provider. Absolutely false. There it is. All providers who are covered entities under HIPAA have to do it. Now that said, the risk analysis that a small, one doc office will do will [differ 00:09:10] greatly from the one that a large hospital system does. The fact still is that you have to do it. It's just it'll vary depending on the size of your organization.

[inaudible 00:09:25] the certified EHR, and therefore that fulfills the security risk analysis requirement, because it's certified. That's also false. Even with a certified EHR, you have to do a security risk analysis. First of all, security requirements address all PHI, not just what's in your EHR. The certification guarantees that the EHR has certain capabilities. It doesn't mean that those abilities are turned on or that they're being used in a way that complies with the HIPAA security rule. Certification does not equal [inaudible 00:10:01] certification. It just means that it has certain capabilities.

[Our 00:10:09] vendor's doing everything to do with privacy and security. I don't have to worry about it at all. Again, false. They can certainly provide assistance. They are doing certain things to address security on their side, especially I come across this one a lot when organizations have cloud-based EHRs, because they think, "Well, all my PHIs over there in the cloud. I don't have any stored on my computers here, so I don't have to worry about it. They're taking care of it." Unfortunately, you are accessing and using the PHI in your office, so it is important that you address that. [As I 00:10:45] said it's your responsibility to do the risk analysis. Sure, your vendor will help with that, and they're doing parts of it, but ultimately it's your responsibility.

I think this is the last one. I have to outsource the risk analysis. I'm not allowed to do it myself. Also false. [inaudible 00:11:04] small practices or even large organizations can do their own risk analysis. Just a caution though, during thorough and professional risk analysis, they'll [spend up 00:11:15] to a complaints review, often that requires expert knowledge that you can get from an outside professional. Oh, one more. I only have to do a risk analysis once. Also false. You need to ... HIPAA requires that you review and

update it regularly. Meaningful use actually specifies a timeline, and says it needs to be done for each reporting period.

Okay, so those are a few myths. I hope we were able to dispel those. Okay. Now what is this thing that we've been talking about, the security risk analysis? Just before I dive into this, I'll let you know there's a lot of content on these slides. Just due to time constraints, I'm going to move through them kind of quickly. If you want to get a little more information and take your time with them a little more as Lori indicated, these slides will be available afterwards.

For starters, what is the security risk analysis? Well, there's no easy answer to that question, unfortunately. There is no single method of best practice or single tool guarantees compliance with the security risk analysis. [Basically 00:12:28] what they have said is do whatever is reasonable and appropriate for your organization. There are a number of tools out there and methodologies. Do whatever makes sense for your organization. Now that said, most risk analysis, risk management process do have certain steps in common. OCR and NIST have provided guidance and recommendations. I'm going to go through some of those commonalities today, so you can kind of see what's coming in a risk analysis.

For those of who come from a medical background out there, I'll put this little bit of medical terms. Just as you diagnose [inaudible 00:13:12] physical data and planned treatments, when you have a chronic disease, you want to assess the risks, come up with a plan, and then continually monitor, evaluate it, and adjust the plan. It's the same for security. We come up with a risk analysis. We look at what are our risks, we [create 00:13:32] an action plan, [inaudible 00:13:34] need to keep reviewing that as we [inaudible 00:13:36] passes and as things change to make sure that we're identifying new risks and adjusting our action plan as we go.

To determine what a security risk analysis is, we have to go through a few definitions. What's a vulnerability? A vulnerability's a thought or a weakness in a system, security procedures, design implementation, or internal control that could be exercised to result in a breach. These vulnerabilities, both technical and non-technical ... A technical vulnerability is pretty easy to understand. I have an un-patched system that has known vulnerabilities in it, weak or no passwords, no encryption on your media just makes you vulnerable to attackers or some other [inaudible 00:14:32] of threat. Also non-technical vulnerabilities. If, say, our users are not aware of current security standards or just don't have a general security awareness, they can easily make that information vulnerable to outsiders. Lack or ineffective policy and procedures, so if we haven't clearly defined how we're using PHI, they do things that put it at risk, put PHI in email, or put on a file sharing site that isn't well protected, or things like that. So there's non-technical things that expose the information as well. We don't want to just focus on the technical.

That brings us to a threat. What is a threat? It's the potential for a person or thing to exercise a specific vulnerability. I included a little clip art on this slide. I'll come back to it a little bit later, too, but I think it's a really good example that kind of puts it in everyday terms. Our vulnerability here is certainly this guy in a little row boat out in probably

what are some very deep waters, and he is vulnerable to flooding and potential drowning. The threat here is obviously this big, huge wave looming over him. He's vulnerable to that threat, exercising his vulnerability, and therefore drowning. That's kind of what we're going to use as our example as we go forward on this.

[Examples 00:16:08] of threats, obviously natural: flood, earthquake, tornado, but also human threats. We include outsiders, the ones we normally think of, the hackers or patients in the office, but also think of threats as workforce members, as these don't necessarily have to be malicious threats. They can be unintentional. Things like [inaudible 00:16:31] modification or disclosure of information. [Perhaps 00:16:35] that person who's sending PHI in an email isn't intentionally putting information at risk, it just may be a lack of awareness or just trying to get something done quickly. This put the information at risk just as much as some of the intentional threats.

I defined those. We can define what's a risk. The net mission impact considering 1: the probability that a particular threat will exercise a vulnerability, and resulting impact should this occur. [inaudible 00:17:11] back to our friend in the rowboat here. He's at high risk of being flooded. Now consider if he were rowing that same rowboat in a tiny little pond in his backyard. The rowboat that he's rowing in would certainly be reasonable and appropriate, because the threat does not exist in that little pond. Now in the ocean, the same little rowboat is not reasonable and appropriate, because the treat is so much higher. You have to consider both the vulnerability and the threat. Putting this into security risk analysis terms, the small SMB firewall that you're going to use in a one doctor office may be very reasonable and appropriate. That same firewall would not be reasonable or appropriate in a large hospital system.

We can see where our security controls have to be evaluated on a case-by-case basis. What is the treat? What's reasonable for my little office versus what's reasonable for a large hospital are going to be very different. That's one things that HIPAA is not prescriptive in its security control. It doesn't say you have to have this, this, and this, because every situation is different. What is the security risk analysis? Again, an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI.

Okay [inaudible 00:18:45] are the different parts of a risk analysis? If we had time I would split these into 9 separate slides, but in order to be concise, I'll just kind of talk to each of these a little bit here on this slide. These have been defined by OCR and NIST. Step 1, I define the scope. [inaudible 00:19:05] very important, and sometimes I think people skim over this a little too quickly. If it's a scope of, let's say that's [inaudible 00:19:12] talking about where you have a cloud-based EHR where you don't have a lot of PHI stored in the office. A lot of people would be tempted to limit the scope to just that cloud-based system. I always step back and say, "You know what? We have to include the local network, because we are accessing and using information on this local network, even if it's not stored here."

If I have a compromised work station that, let's say, has key logger installed, next time I type my EHR password, it's getting sent off to a hacker in another country or something.

We certainly need to be careful when we define that scope and not limit it to much. Similarly, if you have a physician's group as part of a hospital, see if the hospital did a risk assessment, and to what extent did that risk assessment cover your physician's group? I find that often there's a little bit of a grey area there. It's very important to take this step.

Step 2: data collection. Now we're looking at interviewing IT people, office managers, providers, looking at previous risk assessments, getting some technical information, like network diagrams, configuration standards, things like that. [inaudible 00:20:24] all that information we can move to step 3, which is identify and document potential threats, and actually steps 3 through 6 or even 7 [inaudible 00:20:36] organization are often done kind of together. You won't necessarily complete step 3, move to step 4, then move to step 5. You might do these kind of together, but what we want to do is identify potential threats and look at current security measures. What is the firewall we have in place? Do we have an antivirus in place? What are our password strengths? Things like that.

Then you can [inaudible 00:20:59], based on those two, what's the likelihood that this threat is going to occur? If it does, what's the potential impact? If the impact is breach of PHI, usually that's pretty high. Based on those things, we can kind of determine a risk level, and there are certain tools and formulas that can help you kind of punch in the other steps, and it kind of comes up with a risk level for you: low, medium, or high. If you've done that, you can finalize your documentation, and make sure you start to do this regularly. Actually I do have a slide for that last step there.

Continuous risk analysis. A lot of organizations will basically say, "Okay, I'm going to do this once a year. I'm going to do my risk analysis in December every year, and then I'll do it. Then I'll worry about it again next year." Actually, a better approach would be to do an integrated risk analysis, so basically any time you have changes to business operations, technical changes, organizational changes, you want to [step 00:22:05] back and say, "Hey, does this introduce any new risks, or does this change our risk profile at all?" If you have a security incident, changing ownership, technology changes, change your servers or network, or changing workflows, it would be good to revisit that and document that. That is actually required by the HIPAA security rule that you update your risk analysis whenever you have changes. That way when you come to next December, you don't have to look back a whole year and say, "Okay, we have to update all this stuff." Most of the legwork will be done for you at that point.

Also, let's say you made a change in January, you don't have to wait until December to evaluate it to see if you introduced any new risks, which would put you at risk for 11 months. It's important to evaluate these things as you go and update at the end of the year a lot easier, too.

Identify your risks. It's important to have a risk management plan. Take a look at your risks. We're never going to reduce all risk to zero, and that's not the intent here. The intent is to prioritize your risk based on risk level, budget, business drivers, things like that. Take all of that into consideration, and determine what's a reasonable and

appropriate, what's your timeline, and how are you going to address these risks? If there's a risk that you choose to accept for a certain length of time, [you 00:23:27] just have to accept it at that time, document your reasoning behind that, so that in event of an audit, you can show, "Yes, we identified this risk, but here's why we had to accept this for this [inaudible 00:23:38] time."

Here's some resources that can help. Healthit.gov is a great website. They've got [guidance 00:23:49] for mobile device privacy and security, they've got some training games, they've got a really good guide for assessing security in your environment. They do [inaudible 00:24:01] privacy security risk assessment tool that you're certainly welcome to try and use. I'll just add that, as I said earlier that while you have this tool and you can go through it, it will be hard to do a rigorous risk assessment that would stand up to compliance standard just based on using a tool. Even with the tool, it might be helpful to have an outside resource help you, but the tool is certainly there for you to use.

[inaudible 00:24:31] has provided guidance on risk analysis, so you can go read that if you like. Like I said, there's NIST standards. Those standards are very in depth and technical, so they might be a little bit overwhelming for some people, but you're certainly welcome to read those. We [inaudible 00:24:49] your regional extension center to help out. I know I saw some names on my attendee list that I recognized from Pennsylvania, and certainly that's an area that I cover, so I'm here to help if people need resources.

[Links 00:25:09] that contains security trends, recent breach reports, annual threat reports, things like that. I spend a lot of time reading those. I know that most people don't, but those are great resources to say, "Okay, how's the city landscape changed in the past year? What are the current threats? What are people dealing with?" That can help you identify areas that you may need to focus on. The [LCR 00:25:36] enforcement data is a great place to look, because that's our greatest resource for understanding what does OCR expect of us in certain areas. I know Nick is going to talk a lot about these things and get into a little more detail on that. I think that'll be really valuable.

[With 00:25:59] that, I am going to turn it over to Nick.

Lori: Adam, that was excellent information. I'd like to introduce our next presenter, which will be Nicholas Heesters. Nick is a licensed attorney with over 20 years of experience in information privacy and security. Nick is the privacy and security specialist for Quality Insights of Delaware, the regional extension center for the state of Delaware. In capacity he works closely with providers, healthcare organizations, business associates, and contractors. Prior to his current role, Nick maintained a private practice and had management positions leading information technology and security efforts for organizations including IBM and JP Morgan Chase. Nick has served on panels regarding privacy and security topics at many venues. He obtained his law degree from Widener University School of Law shortly after receiving his master of engineering degree in computer and software engineering from Widener University and [inaudible 00:27:05]

as a certified information privacy professional, certified HIPAA professional, and certified HIPAA privacy and security expert. With that, I will hand things over to Nick.

Nick: [inaudible 00:27:19], and thank you, Adam. I want to welcome everyone to the second half of the webinar. I also want to thank Adam specifically for all of his excellent information regarding the security analysis process as part of the HIPAA audits, both the phase 1 audits from 2012 as well as the proposed phase 2 audits, the security risk assessments feature prominently in both of those audit phases.

As far as the HIPAA audits go, just a little bit of background on them, the HITECH act from 2009 require that the government [process 00:28:13] together to conduct audits for compliance with HIPAA regulations. 2012, the first phase, or phase 1 of HIPAA audits was conducted by the Office for Civil Rights, that is the [inaudible 00:28:31] on their health and human services that has the enforcement authority for HIPAA compliance. In 2013, the [inaudible 00:28:40] of that phase 1 of HIPAA audits was evaluated to see what issues were found to be common, to be out of compliance, and might lead to a direction for a more robust and meaningful audit program in the future. 2014, the phase 2 audits were supposed to begin, but they did not. There were several reasons, technical and logistical from what I understand, that the audits were delayed. The audits are scheduled to begin and, to some extent, have begun in 2015. We'll talk about what that means.

[referring to one 00:29:35] who is a potential auditee under HIPAA? The covered entities are going to be healthcare clearinghouses, healthcare plans, and providers. A provider is anyone from a small office, or a small practice, or a dental office, all the way up to large health systems and hospitals. All business associates may also be audited for HIPAA compliance. For the first part of the phase 2 audits was a pre-audit survey that [inaudible 00:30:12] to be mailed to several hundred organizations to gather information about those organizations to OCR in the selection of who they're going to select to audit. Surveys were mailed out in May of 2015. They have already been sent. OCR has been pretty tight lipped about the audit process, but I could image that they have been going through a process of analyzing this data and categorizing the information in order to randomize the selection process for the next portion of the phase 2 audit.

[inaudible 00:31:01] information the audit survey included, what the entity's size was, where other locations were, what sources they provided, what their revenue was, the number of patient visits or insured lives, if or how they use electronic medical record systems, and contact information.

Here's an example of one of the pages from one of the pre-audit survey letters. It was divided into different sections. There were areas in the survey for if you were a clearinghouse organization or a provider organization or a business [inaudible 00:31:44], or a healthcare plan. This particular page, and this is from the provider section, it asks what kind of provider are you, how many [patient 00:31:56] visits in the prior [fiscal 00:31:58] year, how many beds, how many clinicians, do you have PHI, electronic

format, do you have an EMR system, what's your total revenue in the most recent fiscal year? That's only one page or a portion of one page rather of that survey document.

Differences between the phase 1 and the phase 2 audits, phase 2 audits ... Well, first, the phase 1 audits were comprehensive. If focused on many areas regarding compliance with the HIPAA privacy rule, the security rule, and the HITECH act specifically breach notification. Those were conducted by contractor. OCR contracted those duties out to KPMG. KPMG had a document request process via letter, and their receiving and reviewing the requested documents. KP would send a team of auditors on [inaudible 00:33:07] to observe the processes of organization, compare those to the documents, policy procedures that they had [inaudible 00:33:18] reviewed of what was requested, as well as interviewing staff and management.

Now for this next round, OCR had previously said that there were going to be more what they call a "desk audit". That would be more of a document production and internal review by OCR staff of the provided documents for compliance with HIPAA standards as well as supporting documentation an organization should have to show that they are engaging in the activities that the policies and procedures indicate that they are engage in. More recently, OCR has indicated that there may be more on-site visits than they previously thought that there might be, but again, they're being pretty tight lipped about actual numbers, so hopefully we'll get some more information about that process versus desk audits and on-site audits.

The difference is is rather than focus on many of the areas within all of the HIPAA rules that these phase 2 audits are going to focus mainly on definitions of the certain areas that were identified from the phase 1 audits. Rather than focus on all aspects and all specifications and standards in a security rule, that those two audits only focus on a subset of those for this go-around.

OCR has communicated some expectations for when they do begin to submit their letters to begin the actual audit process. If you are selected for an audit, [inaudible 00:35:19] indicate they expect that the documents to be produced, that data requests will be complete [inaudible 00:35:29] specify what the content is to be, and the format [inaudible 00:35:34] requirements of those documents, and they expect those to be followed. Timeliness, only responses that are submitted on time will be considered for the actual audit process. Accuracy: documents that are submitted must be placed in first as of the date of the document request. If an organization received a HIPAA pre-audit survey letter, that would be a good time to review your policies and procedures and other documentation to ensure that it is in compliance with the HIPAA rules. Once [you receive 00:36:24] a letter, you have been selected for an audit. Any documents created [inaudible 00:36:31] of the letter won't count for the audit. They can't be submitted. Documents that are submitted should [inaudible 00:36:42] extraneous data within the documentation that might make it more difficult for an auditor to assess, to properly assess what's actually been submitted. Accuracy: OCR wants the data to be accurate because, as indicated, there won't be as much of an opportunity as the phase 1 audits to engage or otherwise ask questions or communicate with an auditor.

Now for the phase 2 audits, instead of all of the different rules for each individual organization, they have indicated that they would [inaudible 00:37:29] auditee to be audited for a particular rule, focus on the particular subsets of that rule. For the security rule, the focus is going to be on the risk analysis. Adam just did an excellent job going through what it means to do a risk analysis properly and correctly, and how to properly document that and make sure that it's current and up to date. I'm not going to really go through that again, just [inaudible 00:38:01] to say that the risk analysis is a key part of one of the first areas if an organization will be selected for a security rule audit.

[inaudible 00:38:18], which Adam has already gone over. Another focus was indicated to be the risk management process, [inaudible 00:38:32] process whereby after conducting a security risk analysis that a risk management plan is put together to mitigate the deficiencies or risks that have been identified by the risk analysis process. Again, Adam has already spoken to the risk management process. I'm not going to repeat his part of the presentation, but then this is an area that's very important for compliance, for the security rule, and now I'll just refer to Adam's material and my material here as a little duplicate of his material, but the risk management process is the other area of significant focus for security rule audit.

Those risk management considerations, the one you're looking at, the risks that are identified and what is the most reasonable and appropriate way to mitigate those risks. [inaudible 00:39:41] HIPAA says to take and into mind, and these include what is the size and the complexity and the capabilities of the systems? What is the organization's ... What is their technical infrastructure, their hardware and software, security capabilities, and what is the costs of implementing these changes to increase security? Overall, what is the probability and criticality of the potential risk to PHI overall for mitigating these different risk areas?

Now, I also have a little bit of information that I wanted to include that references some of the resolution agreements. These would be the enforcement activities that Adam referenced. I was going to talk about what happens when an organization does not follow what is requested within an audit process that we're talking about to be in compliance with HIPAA. From a risk analysis standpoint, it's relatively recent Anchorage Community Mental Health Services December 2014, they had a breach and investigation. As a result of that investigation, OCR indicated that [inaudible 00:41:12] failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality and integrity and availability of PHI, and that they failed to implement policies and procedures, to implement security measures that would reduce those risks and vulnerabilities to a reasonable and appropriate level.

It's pretty much right there. That's really the definition of what it means to conduct a risk analysis and to have a risk management plan. These are things that ACMHS just didn't do, or at least that was the finding of the OCR investigation. Part of the settlement ACMHS agreed to pay $150,000 [for 00:41:57] deficiencies.

Affinity Health Plan, I believe are up in New York somewhere, [again 00:42:05] failed to assess and identify potential security risks, in this case, this is regards to PHI stored on

photocopier hard drives. This has been talked about a little bit in recent times especially for [inaudible 00:42:21] that leased their copier systems, ensure that if you work with vendors, and make sure that there is a process to ensure that any data that's on those hard drives is appropriately wiped or that you purchased a hard drive and properly disposed it yourself because of the risk of breached date and [lack of 00:42:46] risk assessment for AHE. Their [inaudible 00:42:51] agreement they ended up paying OCR 1.215 million dollars.

[Idaho 00:43:00] State back in 2013, the investigation by OCR said that they did not conduct analysis of the risk to the confidentiality of PHI as part of [security 00:43:10] management process, security management process for about five years there, and did not implement security measures specifically to reduce risks and vulnerabilities. Because of this process, again, not properly conducting risk assessment to identify these risks, not having a proper risk management process to reduce identified risks. As part of their [inaudible 00:43:36] agreement, they paid over $400,000.

[All right, 00:43:42] a privacy audit. If someone is selected for an audit that focuses on the privacy rule, one of the areas of focus was indicated to be the notice privacy practices. This is how a covered entity [would 00:43:58] use and disclose PHI, talks about individual's rights, with respect to that information and how they may exercise those rights, and what the covered entity's legal duties are [inaudible 00:44:10] to that information. Make sure that the NPPs are in place, [inaudible 00:44:18] to get a signed acknowledgement from the patient that they have read and acknowledged, received a copy of those NPPS, and that there were updates prior to NPPs as a result of the Omnibus rule in 2013. They would want to see a copy of NPPs to make sure that they did include the updated Omnibus information.

[inaudible 00:44:49] focus, that as [inaudible 00:44:51] indicated that we'll be looking at if for a privacy rule audit would be patient access to the health records. OCR has on several occasions indicated that they take a patient's right to access his or her health records very seriously. That is an integral part of the privacy rule, which extends to the electronic environment. Now individuals do have that absolute right, with exceptions to obtain copies of their PHI. For this one, OCR would most likely be looking for policy procedures regarding how to provide access to medical records to a patient if requested, or a personal representative requested it, if there's any kind of documents that a person would have to fill out to get access to those records, and what the internal review process would be like to show that they access was granted and patients did in fact receive those records. That would indicate supporting documentation that the patients were able to receive access to their health records.

There's a going a little bit an older one here, 2011. There was an issue with a health plan not providing health records. Cignet Health, and this was taken from the Civil Monetary Penalty letter, which notified Cignet Health that they should provide 41 individuals timely access to their copies of health information, and the [inaudible 00:46:46] record sets that Cignet maintained, that there were violations of various HIPAA regulations. Because of those violations, the last part of that is there on the second bullet point that I'm going to inform you the monetary penalty of $4.351 million against Cignet Health is

final. That's one of the larger fines that has been opposed on an organization for HIPAA violations. That was for failure to provide access to health records.

Another focus on the HIPAA audits would be on the HITECH act, specifically on breach notification. There were some changes on what it means to be a breach and have what is a presumption of a breach that any impermissible use of [inaudible 00:47:46] PHI is now presumed to be a breach under the Omnibus rule. There are certain exclusions, which are listed there. For one, OCR would want to look at your breach notification policy and procedures to make sure that they have been appropriately updated versus the [interim 00:48:10] final breach notification procedures, which the Omnibus [inaudible 00:48:15]. I'm sure those updates are appropriately reflected in [inaudible 00:48:20] policies. [inaudible 00:48:23] is the risk analysts process is a totally different now that four factor risk assessment, the review, make sure [inaudible 00:48:36] PHI involved in the breach, to whom that information was disclosed, was the PHI acquired or viewed, and what steps were taken to mitigate that disclosure.

Any kind of documentation that is going to document the process, this four factor risk assessment that the organization went through to make a determination or not a breach was reportable, and going through [inaudible 00:49:07] this assessment, if it could not be determined that there was a [inaudible 00:49:15] breach, that there was not a compromise of health information, then it would have to be reported. What your determination was and how you used assessment to make a determination is [possible 00:49:30] the documentation they would want to see to be compliant with them as part of the audit. Safe Harbor for the portable [inaudible 00:49:41] is going to be for electronic PHI, destruction and encryption, paper based PHI, another electronic is going to be destruction. Just again, [inaudible 00:49:57] that I'll look for to make sure that those policies are in place, that they've been updated with the Omnibus [inaudible 00:50:02]. If there has been a breach and letters and notifications were sent out, they want to see copies of those letters, kind of activities surrounding a breach, and [inaudible 00:50:16] of the breach.

A couple breach issues. Skagit County, Washington failed to provide proper notification had to pay $200,000. Adult and Pediatric Dermatology did not comply with requirements of the breach notification rule, did not have written policy and procedures, did not train members of the workforce regarding breach requirements, had to pay $150,000.

As far as some other areas that [inaudible 00:50:50] look at for audits in the future: device and media controls, need a secure, need a reuse disposal accountability for PHI and devices, data backup and storage, transmission security with encryption and integrity controls, and from a privacy standpoint safeguards for PHI in your surroundings, physical surroundings, how to secure paper or other non-electronic PHI physically, or whether it's written or verbal, and [inaudible 00:51:25] make sure that everyone is properly trained in an organization's policies, and that the supporting documentation of training, training materials, and attendance records.

These were identified as future areas, [inaudible 00:51:39] and the overall beginning of the audit process, there have been some [rumblings 00:51:44] that future items might make it into the phase 2 audit process. Have to see OCR send out their first letters of that will be the case or not.

Director [inaudible 00:52:01] Samuels, one of her first media briefings earlier this year stressed several areas of HIPAA compliance, and these are areas that she says her team has seen repeated deficiencies in in her investigation and, again, comprehensive risk analysis and risk management practices at the top of the hour, those are all the things that Adam talked about. [inaudible 00:52:25] begin my presentation. This is going to be a focus on the security rule audits. This is a huge area that [inaudible 00:52:32] really look in to make sure that people do this and do it right, ignoring frets and hazards. If you do your risk analysis, you have frets and you don't do a thing about it. Your frets are not mitigated as part of your risk management practices. That's an identified issue. Having policy and procedures, not having supporting documentation is a continuing issues, and training of workforce members in those policy procedures is also a continuing issue.

[inaudible 00:53:00] a refresher in civil enforcement, $100 to $50,000 per breach. Per breach is per record, not per breach issue. If a breach impacts 10,000 records, that is $50,000 times 10,000 records. It is not just $50,000 for the entire breach. Criminal penalty's $50,000 to a million dollar fine, and 10 years in federal prison. It's just used for healthcare fraud, but there's a doctor in UCLA medical center that was sentenced to four months in federal prison for [inaudible 00:53:42]. They do look at other areas outside of healthcare fraud from time to time. Of course on the HITECH act, attorney general are now permitted civilly sue an organization on behalf of effective state residents.

Resources, and this is ... I think Adam had a similar list at the end of his presentation quality insights. As I've indicated, we assist organizations with the risk assessment processes. We do that here in Delaware and Pennsylvania, West Virginia, and some other states. I think we have ... I am going to [inaudible 00:54:26] the session over to Kathy Rivard for some closing areas there for the [inaudible 00:54:35].

Kathy: Thank you Nick and Adam for sharing all this information. There are so many requirements. It's very difficult to get all of this straight. I'm sure all of our practices in our 5 states benefited from hearing about this. As Adam mentioned, he's based out of Pennsylvania, Nick, you are in Delaware, and we also have a staff member in West Virginia that can assist those practices. For those of you on the call today from the state of New Jersey, [inaudible 00:55:06] some contact information. The New Jersey Health Information Technology Extension Center, which is formerly the Regional Extension Center has privacy and security services available. You do not have to be [inaudible 00:55:22] there. You can reach out to the director, whose name, even though he has a long name, you can call him by "Valla". His website address or the New Jersey HITECH address is there, and you can reach out to them if you'd like to get services if you are in New Jersey.

If you are a practice located in Louisiana listening to this call, the Louisiana Health Information Technology Resource Center also offers privacy and security services for all the practices in Louisiana. The telephone number to call there is 225-334-9299, or you can email them also if you'd like some assistance.

[inaudible 00:56:13] is just, once again, our 5 states, we have a contact person in each state. I know we are running really short on time. We'll see if we have time for one or two questions. If not, please reach out to the contact in your state with any privacy and security questions, and we will make sure that we get to Nick and Adam and get those questions answered for you.

Lori: Kathy-

Kathy: I'm going to go ahead and turn it over to you to see if we do have time for one or two questions.

Lori: Absolutely. Thanks, everyone, for your wonderful presentations. If you have submitted a question in the chat feature, we will address it now, or if there's anything that comes to mind, please feel free to type that in the chat window for the next couple minutes here. We did have a question submitted, so I'll go ahead and read that. As a health group, does our security risk analysis need to be personalized for each individual provider's office, or can we use the analysis that looks at our group as a whole?

Adam: I'll answer that. What I generally do, I'm assuming they're referring to an organization with multiple locations. What I usually find is a lot of the policies, procedures, technology, things like that are common across the locations. There is no requirement that you do a separate risk analysis for each location. However, what I do is I generally [inaudible 00:57:48] analysis that includes kind of the common answers for everything that's the same across locations. Things like physical security or some specifics on how they handle patient information in some of the clinics or offices, then I will fill out separate sections for each office. The overall assessment is just one, but there may be specifics for each location.

Lori: Thanks, Adam. We have another question. What's considered timely access to health records for our patients? We offer to everyone a patient portal, but some still refuse that service and rather paper health information.

Nick: Well, [inaudible 00:58:39] 30 days. There is 30 days to give them access to their information, and there is a 30 day extension period. That is to take advantage if, say, some records are in storage off site somewhere, and some time that is required to retrieve that data [inaudible 00:58:59] that additional time in there to be able to [inaudible 00:59:06] activities.

Lori: Okay. Another comment was, "I understand that a security risk assessment tool was developed by ONC, the Office of Civil Rights, and the Office of General Council, and it is available on the healthit.gov website. I have a small practice with only two physicians. If

I download that tool and answer the 156 questions, will I meet the privacy and security requirement for Meaningful Use?

Adam: Well, I've learned that I can give a lot of guarantees in this business. Yeah, you can't guarantee the answer's yes or no. It's a tool to help you do it, and it certainly can be used, if it's used in good faith to meet the requirements, but like I said, it's a tool. You can't guarantee that just because you answered the questions you are going to meet the requirements.

Lori: I'm trying to meet Meaningful Use for calendar year 2015. Do I need to have the privacy and security assessment done by December 31st of this year?

Nick: Well, the [inaudible 01:00:31] but there is some [inaudible 01:00:32] out there that indicates that having it done after the 31st will be okay. In particular, there's an FAQ, and I don't have the FAQ number in front of me, but on CMSs website they did indicate that conducting a security risk analysis for a Meaningful Use period is acceptable any time from January 1st from when that period begins up until the actual date for which you are required to submit your [attestation 01:01:10]. In as much as if you can't submit your [attestation 01:01:13], I believe last year and possibly this year up to the end of the first quarter. I have to look at the Meaningful Use rule to double check that, but last year that was the case. You could have your risk assessment from 2015 done within the beginning of 2014 ... Or 2014 it could be done the beginning of 2015, but that risk analysis that was done in the beginning of 2015 can't count two times, so that would not count for the 2014 and the 2015 Meaningful Use [attestations 01:01:56]. You would need to do another risk assessment [inaudible 01:02:01] in 2015 or early 2016 to meet the requirements for the security measure for the 2015 Meaningful Use requirement.

Lori: Thanks, Nick. I think we are now out of time. Thanks to all of our speakers, and thank you, everyone, for joining us today to learn more about the security risk assessment. If you have any additional questions, please reach out to your local quality insights team member. That information was listed on the screen and will be included on the power point that we post on the website. Please [inaudible 01:02:36] that theses slides and the recording of today's event will be on the website, and that web address, again, is www.qualityinsights-qin.org, and it will be listed under the events tab as an archived event. There will be a very brief evaluation at the close of this session, so we encourage you to please take just a moment to complete it. It really [inaudible 01:02:59] help us plan for future events to get your feedback and input. With that, I'd like to thank you for taking the time out of your day to join us for this session, and have a great day.