The Security Risk Analysis Requirement for MIPS
Transcript from Live Webinar

Tuesday, August 8, 2017

Shanen: Good afternoon and welcome to today's webinar, The Security Risk Analysis Requirement for MIPS. My name is Shanen Wright and I'm an Associate Project Director for Quality Insights' QPP Support Center. I will be serving as the host for today's session and Communications Specialist Laurie Fink will be producing the event. We will get started with today's program in just a few moments, but first, a few housekeeping items.

All participants enter today's webinar in a listen only mode. Should you have a question during today's presentation, we ask that you please type it into either the chat or the Q&A box to the right of your screen. We will answer as many questions as we can at the end of the program. Today's webinar is being recorded. The recording will be posted on the Quality Insights website as well as the Quality Insights QPP Support Center website later today.

You should have received a copy of the slide deck for today's presentation earlier this morning via email. But if for some reason you did not, I will send all of you a link to where these resources are posted as soon as they are available. It is now my pleasure to introduce you to today's speaker, Greg Fink.

Greg has worked for Quality Insights since 2004, and became our primary security subject matter expert to better serve our customers and partners. So, without further ado, I will now hand over the presentation to Greg.

Greg Fink: Thank you very much, Shanen, and good afternoon to everyone. Thank you very much for taking the time to join us for this important webinar on The Requirement of a Security Risk Analysis for MIPS. Next slide, please.

Our agenda for today includes the HIPAA Security Rule and how to conduct a Security Risk Analysis. We will discuss the security areas to consider, including a physical safeguards, administrative safeguards, and technical safeguards. Next we will discuss policies and procedures, followed by an overview of the security risk assessment tool and where to find it. I will also provide links to valuable resources and then we will leave time for questions at the end. Next slide, please.

Let's get right into it. Under the HIPAA Security Rule, you're required to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. Once you have completed the risk analysis, you must take any additional reasonable and appropriate steps to reduce the identified risks to reasonable and appropriate levels.

The HIPAA Security Rule requires healthcare providers, health plans, and business associates to conduct risk analysis and implement technical, physical, and administrative safeguards for electronic PHI. In order to score any points for the Advancing Care Information category of MIPS, a Security Risk Analysis must be completed during the reporting year. Next slide, please.

How to Conduct a Bona Fide HIPAA Security Risk Analysis. There's no single method or best practice that guarantees compliance, but most risk analysis and risk management processes have the same steps in common. A common question is, "Do I have to outsource the security risk analysis?" The answer is no. It is possible for small practices to perform a risk analysis themselves using self-help tools. However, the risk analysis must be thorough to pass a CMS audit. You may need a professional to assist you with the physical and educational safeguards of protection the patient's electronic PHI. If you have an IT professional in your practice, they should be able to assist with the security risk analysis. Next slide, please.

Points to ponder and think about. There's always a right way, but there's also wrong ways. An initial security risk analysis requires a lot of time and work because there is a lot of information that must be collected. The security risk analysis is not a once and done task. It needs to be updated and protected. It is one of the single biggest audit and investigation findings and always requested in an Office of Civil Rights enforcement action. Next slide, please.

Performing a Security Risk Analysis. So, how do we do this? Next slide, please.

Important First Steps. Establish a comprehensive information security program. Make sure everyone is on board and takes this seriously. Designate an accountable Security Officer. Develop privacy and security policies and procedures for everyone. Distribute and update policies and procedures to everyone. Document authorized access to electronic PHI and continue to educate staff. Next slide, please.

Also, document processes for responding to security incidents. Test your processes, if possible. Implement training and sanctions for non-compliance. You have to get the message across that this is a big deal and it can be costly. Conduct a risk analysis. Establish risk management process. Implement reasonable safeguards to control risks. Place the high priority items first. Develop a Disaster Recovery Plan. If you can test it, test it. Always keep employees on their toes. Next slide, please.

Also, regularly review records of information system activity. Find out who utilizes your system. Implement reasonable steps to select service providers. Test and monitor security controls following any changes to the system. Obtain assessments from qualified independent third parties and also assess their security. Next slide, please.

Three important terms to remember. Number one, reasonable diligence. The business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances. Taking reasonable care of electronic PHI and keeping it safe. Number two, reasonable cause. An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act of omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect. Mistakes are made. Taking the steps to avoid them, having the response to minimize them, is the best practice. Next slide, please.

Number three, willful neglect. Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated. Conscious, reckless behavior is a no-no. Knowing that you needed to fix that door lock and didn't, someone broke in and stole all the computers. That is willful neglect. Next slide, please. As you can see, it can be very costly and it could be devastating to your business. Next slide, please.

The Security Management Process. You are able to implement specific policies and procedures to detect, contain, and correct security violations. Risk analysis. Conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. Next slide, please.

What a Risk Analysis is. It is the process of identifying, prioritizing, and estimating risks to organizational operations, which includes the mission, the functions, image, reputation, organizational assets, individuals, other organizations resulting from the operation of an information system. Part of the risk management incorporates threat and vulnerability analysis and considers mitigations provided by security controls planned or in place. Next slide, please.

What a Risk Analysis is not. A network vulnerability scan, a penetration test, a social engineering test, a configuration audit, a network diagram review, information system activity review, SOC 2 or SOC 3 report, intrusion detection. It's all of these. Next slide, please.

ONC, the Office of National Coordinator, Guide to Privacy and Security of Electronic Health Information. In conjunction with OCR, the Office of Civil Rights, the Office of National Coordinator developed a risk assessment guide. The risk analysis is the process of identifying, prioritizing, and estimating risks, considers mitigations provided by security controls planned or in place. NIST, or the National Institute of Standards and Terminology, SP800-30 is the risk management guide. The link to the Guide to Privacy and Security of Electronic Health Information is on the page. Next slide, please.

How much risk are you willing to take? What is the likelihood something will happen? What would be the impact to the practice if it does happen? Establishing a risk value think likelihood is important. Next slide, please.

What are the results if done properly? You can avoid security incidents or breaches. You will be prepared for HITECH mandatory audits. You will be prepared for an Office of Civil Rights investigation. You will have a solid educational foundation and be able to complete a risk analysis. Next slide, please.

Results if done properly. You will have a solid security foundation. You will be able to create a sound basis for risk management and be able to manage decisions when incidents occur. You will be able to develop a remediation plan, a risk analysis, and produce a remediation report and have a basis for ongoing risk management and protect the continuity of the business. Next slide, please.

When performing a security risk analysis, you need to define the scope of the risk analysis and collect data regarding the electronic PHI. You need to identify potential threats and vulnerabilities to patient privacy and to the security of your practice's electronic PHI. You need to assess the effectiveness of implemented security measures in protecting against the identified threats and vulnerabilities. You need to determine the likelihood that a particular threat will occur and the impact it would have to the electronic PHI and your business. Next slide, please.

When performing a security risk analysis, you also need to determine and assign risk levels based on the likelihood and impact of threat occurrence. You need to prioritize the remediation or mitigation of identified risks based on the severity of their impact on your patients and practice. You need to document your risk analysis, including information, and document the steps you've taken as well as the risk analysis results. You must also review and update your risk analysis on a periodic basis, a minimum, at least once a year. If you have a breach, you have to review it again after the breach. Next slide, please.

When protecting your patients' electronic information, the Security Rule requires that you put into place reasonable and appropriate physical safeguards, administrative safeguards, and technical safeguards. Next slide, please.

What are the physical safeguards? They are your practice and other places where patient data is accessed, computer equipment, portable devices. Some examples are your building alarm systems, your security systems, locked doors and offices, and screen shields that basically shield from secondary viewers. The number one reason for breaches today is lost or stolen assets. Next slide, please.

Administrative Safeguards. It is required that you have a designated security officer nominated. You must also have a workforce training and oversight. You must also control information access and have a periodic security risk assessment performed. Some examples are staff training and education, monthly review of user activities, and policy enforcement. The number two most common reason for breaches today is human error. Education is so very important. Next slide, please.

Technical Safeguards. They are the control of access to the EHR; the use of audit logs to monitor users and other EHR activities; measures that keep electronic patient data from improper exchanges, scans, intrusion detection, antivirus, and secure unauthorized electronic exchanges of patient information. Some examples are to use secure passwords, back up data, antivirus checks, and data encryption where appropriate, especially on servers, laptops, tablets, and phones. Next slide, please.

Policies and procedures are the heart of the risk assessment. Written policies and procedures are necessary to ensure HIPAA security compliance. Documentation of security measures is key. Examples include written protocols of authorized users, record retention, policies for passwords, and policies for education and awareness. Next slide, please.

Organizational Requirements. Business associate agreements are a very important requirement. The Omnibus will also make sure that business associate agreements are as responsible as covered entities for any incidence. Create a plan for identifying and managing vendors who access, create, or store electronic protected health information, document the agreements, review them, and update them. You must have business associate agreements documented and updated with any third party that touches the electronic PHI. Next slide, please.

When performing a risk analysis, you must demonstrate a good faith effort and also exercise reasonable diligence. Next slide, please.

The Security Management Process Standard is one of the requirements in the HIPAA Security Rule. Conducting a risk analysis is one of the requirements that provides instructions to implement the security management process. The Office of National Coordinator worked with the Office of Civil Rights to create a tool to help guide healthcare providers from small practices through the risk assessment process. Next slide, please.

The Security Management Process Standard includes the security risk analysis tool. Use of this tool is not required by the HIPAA Security Rule, but is meant to help provide helpful assistance. There's a link for the security risk assessment tool. The link is also provided on the QPP website. Next slide, please.

So, let's get into the security risk assessment tool. It's found on HealthIT.gov website as well as Quality Insights website. As you can see, it basically provides you with information and instructions on the security risk assessment tool. The security risk assessment tool takes you through each HIPAA requirement by presenting a question about your organization's activities. Your yes or no answer will show you if you need to take corrective action for that particular item. There are 156 questions, so completing it is time consuming. That is why you should get started right now if you haven't completed one in the past. Next slide, please.

The first step is to download the security risk assessment tool. For those of you who would like a printout, you can also print the paper based version. Next slide, please.

You should also download the Security Risk Assessment Tool User Guide. It provides very helpful directions. Next slide, please.

It is also recommended that you watch the tutorial. This is a very helpful tool for you that will help you throughout the process and answer all the questions about information that is needed in the security risk assessment. Next slide, please.

Here is a screenshot of part of the tool. One thing I want to stress is the importance of saving the tool while you are completing it because if you don't save it, you will lose it and have to start over. Next slide, please.

Here's the Security Risk Assessment Tool Home Page. It is very easy to follow. Question number one is “Does your practice develop, document, and implement policies and procedures? “ You can see right below current activities, it lists activities you may have done or are working on towards achieving a yes answer. Do you have documented policies and procedures? If not, you can see at the bottom, it's necessary to mark low, medium, or high. If you don't have documented procedures, that's a high impact. What have you done? Steps you've taken to remediate that threat. Also, note the helpful information on the right side. Next slide, please.

As you can see, top right, they have little tabs. The second tab is Threats and Vulnerabilities. It also lists examples and gives you important information. Next slide, please.

Tab number three, Examples of Safeguards. These are key examples that you can utilize for your practice. Now, the way that this was set up was basically for large practices, so small practices may not need a lot of this information. Next slide, please.

As you can see on the bottom of the page there are options. Remember, there are 156 questions, so take your time and answer the questions to the best of your knowledge and be truthful. When you are done, you will have a report that shows you what you need to work. You can utilize the navigator to go back and forth throughout the whole process. Also, you can type in related information and export data. Next slide, please.

This is basically what it looks like when you input information. It provides you with answers, you can flag items that you need to work on, it shows your risk level, it shows current activities, notes, and also more importantly, what remediation steps you have taken. Also important is the last edit date, when you were in the tool. This is very important because if you don't use the tool and you get audited, the auditor will see the previous dates and that could hurt you. Next slide, please.

This is a fun little guide here in that basically it shows you, once you start putting information in, it will give you a reading. It'll give you a picture of where you are, and the amount of low, medium, and high risks that you have. Next slide, please.

Once again, this shows basically your security risk analysis report. Again, it's only as good as the information you enter into the tool. You need to be truthful. You can't just run through the questions and check yes for everything. You want to make sure that you have all bases covered. It won't help you to enter a yes and then not work on any of the vulnerabilities in the event of a breach or disaster. Next slide, please.

So, start now. Don't wait. Do it now. Next slide, please.

Also, don't forget the security risk analysis is not once and done. You want to make sure that if you have any vulnerabilities, you list the high priority items, get them done, and take care of them as soon as possible. It is acceptable to be working on medium and low weight items. If you're considering vulnerability testing for your system, which a lot of organizations do, you can look into different vulnerability systems or software for your system. That takes time. So, you want to make sure that you document that you're doing that if that's one of the vulnerabilities. Next slide, please.

What happens after it's finished? You must keep an eye on security. You must update and educate. You must document everything, and also discipline if you have to. Next slide, please.

Keep an inventory list. Keep checklists. Walk through checklists, checklists on things that you need to have done. Demonstrate good effort and exercise reasonable diligence. Next slide, please.

A little bit about the HealthIT.gov website. As you can see, bottom center, you can see Privacy & Security is listed. That's where you need to go for some helpful resources. Next slide, please.

You can see the tab Privacy & Security and basically click on that tab. Next slide, please.

Once you click on the tab, you can see the available resources down the left hand side as well as in the middle. Close to the bottom, you can see Privacy & Security Training Game. This is a nice, fun game that everyone can use, even employees. Basically it takes you through the office and gives you scenarios that you can actually get graded on. You can also grade on the improvement of your staff. I just want to mention briefly, cybersecurity, right underneath Privacy & Security Training Game, is on a lot of people's minds because there's been a lot of talk about it. Ransom ware is a national problem and becoming a healthcare problem. So, you want to stay safe. Next slide, please.

Here are some Health IT links. Number two, Information Security Policy Template, can be utilized for your policies and procedures. Then right below is the Security Risk Assessment Tool that you will be using. Next slide, please.

Here are some more links that you can utilize, such as the Guide to Privacy and Security and Health Information Privacy, Security, and Your EHR. Next slide, please.

And here are more online resources. There is a Security Risk Analysis Tip Sheet that has been used for the EHR incentive programs which is very helpful. Also, there is a summary of the HIPAA Security Rule. HIMSS produces great resources for privacy and security. Also, there is the National Cyber Security Alliance, and Stay Safe Online produces some very nice resources. Every October is Cybersecurity Awareness Month and they usually produce some documents and pics to Stay Safe Online. Next slide, please.

Lastly, Quality Insights Can Help. If you go to our QPP Support website at www.QPPsupport.org or call us, we can provide free QPP assistance to you. Next slide, please.

Lastly, thank you very much for attending today's webinar. We now have some time to answer your questions.

Shanen Wright: Thank you Greg. At this time, we will move into the Q&A portion of the session. If you have any questions for Greg, please feel free to type them into either the chat or the Q&A box on the right of your screen. If you have already submitted a question, which I did see several questions already in there, during the presentation, we will address all those questions now as time permits.

I will go ahead and start reading you some of the questions that have already been submitted. The first question asks, "If you completed a security risk assessment in 2016, can you just update it for 2017?"

Greg Fink: Yes. The rule states that you can conduct or review a security risk analysis. So, it definitely needs to be reviewed every year once it's conducted.

Shanen Wright: So, basically they can just update it. They don't need to create a whole new analysis?

Greg Fink: No, they don't. They just have to make sure that they document any changes they've made since the previous year. The tool that's provided, actually you can see where we went over, you can basically use that and put the dates in there that you are basically addressing vulnerabilities.

Shanen Wright: Okay. Can you start and save it or do you have to finish it all in one sitting using the tool?

Greg Fink: You can save it as you go. Just make sure you save it before closing.

Shanen Wright: Okay. The next question is, "We lease our office space. Although our office is locked when we are not here, the main lobby of the building is often unlocked for the other tenants. I also am unsure of the landlord's security as far as cameras, etc. What action should we take?"

Greg Fink: Okay. First of all, you want to make sure that if you don't own the building, you have the proper insurance. If you have any type of computers that are server based, you want to make sure that all of the rooms are locked and basically all of the computers are locked up, all of the assets are locked up. Also, if that's the case, you should probably make sure that all of the computers are encrypted for extra security.

Shanen Wright: Okay. Next question is around the same topic. It says, "So, we created an account and it saves all of our information in the tool. Does the tool submit that information anywhere or do we just need to export it and keep it for our records?"

Greg Fink: Yes. Basically, you just need to export it and keep it for your records just in case you get audited.

Shanen Wright: Okay. "If we are attesting to just one quarter for MIPS, does the security risk analysis have to be completed during that quarter or can it be completed before or after?"

Greg Fink: The security risk analysis can be completed any time during the calendar year. It does not have to be done during the quarter when data is collected and reported. You cannot utilize a risk assessment from a previous year. It must be conducted every year.

Shanen Wright: All right. The next attendee asks, "So, if we had a professional do our security risk analysis the last three years, can we just update it with dates and what we did?"

Greg Fink: Yes you can update it. As I mentioned before, if there's any changes, let's say in the workforce or if you had a change of systems, that might be all that needs to be addressed. Also, you need to make sure that the threats and vulnerabilities that were in the previous three years are not still lurking around and have been addressed. A lot of people carry them from year to year to year and don't do anything. If you're going to update it, you want to make sure that you address the vulnerabilities appropriately.

Shanen Wright: All right. The next question asks, "If we download and utilize the tool, will it be sufficient if we are audited?"

Greg Fink: If the tool is done thoroughly and there are no extenuating circumstances, meaning that if there's technical issues, namely servers, that are not addressed and issues that are not addressed, let's say security issue, they're going to be still liable. You want to make sure that all of those are addressed. But they are in compliance.

Shanen Wright: Okay, great. "Is the practice also responsible for the computers that are placed in the office for blood work input? We already have individual logins for each personnel accessing the system."

Greg Fink: Yes. You definitely need to be able to check passwords and change passwords and any patient information that is on any type of asset in the office is or could be a liability if that information is basically stolen. So, it needs to be protected. Encryption is the best way to protect it.

Shanen Wright: Okay. This next question is a great follow up to that answer. It asks, "What are good options for data encryption?"

Greg Fink: There are many options for you online for data encryption. Basically, that's the best way to keep the information safe if the asset is stolen.

Shanen Wright: Okay. Another question is from someone who is an IT professional and they are looking at the security risk analysis from more of a technology standpoint. So, firewalls, AV, BYOD devices. What do you recommend as far as that goes?

Greg Fink: This is just basically a tool that provides 156 questions. It's the responsibility of the practice and the IT personnel to evaluate all of those different assets and basically vulnerabilities. So, it's up to them to basically provide options. There are a lot of options for, let's say even vulnerability scans, encryption, antiviruses.

You have options that you could go online and do a Google search. Basically, whatever is cost effective for your practice. Remember, there's a risk associated with basically not utilizing that software. Let’s say a vulnerability scan that scans the system monthly or every three months. There's a risk there. If you have good encryption, it minimizes those risks. So, it's basically up to the organization and the IT personnel if they have them to basically work up a plan and utilize some of the software for their own protection.

Shanen Wright: "Is there any way to submit the security risk analysis that a practice does to the Office of Civil Rights so that it can be approved and the practice knows that they are covered?"

Greg Fink: That's a good question, but I don’t believe the OCR will review an analysis. I think if you have an experienced IT professional, you should be fine. The Office of National Coordinator is looking for organizations that do not comply with the analysis. If you have any threats or vulnerabilities, the best thing to do is contact an experienced IT individual that can provide you with options for the threats or vulnerabilities.

Shanen Wright: All right. Our next question asks, "What happens if we finished our annual security risk analysis review and then changed our medical billing system?"

Greg Fink: Basically, that would be on a new system, so I would reevaluate your security process. Depending on the third party that's involved, you may need to have a new business associate agreement and/or address agreements. So, you should probably reevaluate the whole risk analysis at the time of the change.

Shanen Wright: Okay. "If a practice had Quality Insights complete a privacy and security risk analysis in 2011 and 2012, will an annual update to that document meet the 2017 MIPS requirements"

Greg Fink: Yes. An annual update or review will satisfy this. But remember that threats and vulnerabilities must be addressed; you can’t just keep carrying them over. If you do not do due diligence and address them and something happens, you're still liable. So, it's a lot easier if you conduct a new analysis or review it. You just want to make sure that you have all bases covered.

Shanen Wright: Okay. Our next question is, "What if employees are on the web doing personal things during work time? Yes, they are not supposed to be browsing, but can they open us up to viruses with our medical software program? Should it be zero tolerance for internet usage in the office?

Greg Fink: This most definitely opens you up for all kinds of bad things to happen. That's how ransomware starts. It starts with emails and opening up those emails. Make sure you have a policy and procedure for employees not to go online unless they have to. For example, if they need to for insurance purposes or something else work related. That will keep the organization safe.

Shanen Wright: Okay. "Who should get the business agreement? How should they be sent out and is there a simple example of one for a small practice?"

Greg Fink: Yes. There are examples of business associate agreements that ONC created for organizations that you do business with. One example is a shredding company that shreds your data. You need a business associate agreement from the shredding company and it needs to be kept on file. Basically, they're required to provide you with a business associate agreement because if they don't, they're just as liable as you for a breach to your records.

Shanen Wright: The next question asks, "What is the best way to handle employees that work remotely?" I guess in regards to browsing the internet or using the computers for personal reasons.

Greg Fink: The best way is encryption and also a VPN, virtual protected network, that they have to log into. But also more importantly, you need someone to basically check to see, they have to check the logs. Who's logging in? When? That needs to checked routinely. Management needs to ensure that there's a vulnerability scan or intrusion detection from the outside. But more importantly, if it's encrypted and they have a virtual protected network, that's probably the best way to go. Also, make sure your practice has policies for working remotely.

Shanen Wright: Okay. Next question is, "Where do I start? What is the first step I should take to develop an assessment for my practice?"

Greg Fink: The first step is to download the tool, then get together with management and generate policies and procedures. Next, review the policies and procedures with everyone in the office and talk about ramifications if there is a breach or if someone causes a breach, and what the penalties are. Make everyone responsible for the safety and security of the patient information in your practice.

Shanen Wright: "How often do business associate agreements need to be updated?"

Greg Fink: If you're working with the same organization for several years and nothing changes in your procedure with them, then you're fine and the BAA doesn't need to be updated. Just be sure that you have an agreement on file with everyone.

Shanen Wright: Okay, there's another question about the business agreements. "The practice does not need to send out the agreements. Did I get that correct? The businesses that we work with should send the practice agreements to us?"

Greg Fink: Correct. They should have a business associate agreement that you fill out with them. Now, if that's not the case, then you could get an agreement and give it to them to sign. If they don't sign, then that's a problem. But they're required to provide business associate agreements. I guess you could report them to the Office of Civil Rights and they may force them to write an agreement.

Shanen Wright: "Do I need to educate my staff more than once a year or once we go over it once, are we covered for that?"

Greg Fink: This will be based on an evaluation of your staff. Usually, most practices do it once a year. But with all of this ransomware going on, it's good to update the staff more frequently. Organizations such as HIMSS and Stay Safe Online have information on their websites regularly. One thing you could do is provide monthly newsletters to the staff. But more important, they need to understand that this is important and that they need to stay safe online and follow the rules so that if the staff knows that, understands that, a couple times a year is better than once a year. But if they're educated on the newer viruses or the newer ransomware that's out there and staying off of the social media type areas, they just need to know the rules and follow them. But more importantly, if they understand this and basically are following the rules, usually once a year is okay. But good practice is more than once a year.

Shanen Wright: Okay. "To clarify, if a business associate hosts software for practices, who is responsible for providing the agreement? The business associate or the practice? Is there a policy that can be referenced for this?"

Greg Fink: This question refers to a web-based organization that is securing their information. You need to have a business associate agreement with them. They should provide you with a business associate agreement. However, you want to make sure that you review what happens if there's anyone trying to get into their system from their end. Also, the practice needs to review who's logging in from our end onto the web-based system. So, basically, the answer to that question is the web-based software organization needs to come up with the BAA. But you need to protect both ends: the user logs of who's using the system as well as on the software vendor's side. They need to provide a report with information on who if there is an intrusion detection.

Shanen Wright: "What policies and procedures do I need if I am connected to a local hospital?"

Greg Fink: If you're connected to the hospital, the security of your assets if they're connected to the hospital, security of the facility, as well as if there's any information transmitted from your end to the hospital end. There needs to be an agreement on the security of that information on both ends. So, there needs to be a business associate agreement from the hospital as well as from your end. You want to make sure that all of the electronic health information is protected. Again, create policies and procedures for staff and the requirements for passwords. And make sure you provide education about policies. If you complete the security tool, you can utilize most of those.

We did not talk about incident security response a lot, which is how you're going to respond, as well as disaster recovery. If there's a disaster in the building that you're connected to, you need a policy for a disaster recovery where you would set up an alternate facility. So, there are definitely some separate policies that you would need to develop. You still have to coordinate those policies and procedures with the hospital, then make sure that you're protected from your end and any connection to the hospital.

Shanen Wright: "Do I have to report a very small incident like a fax being sent to the wrong person?"

Greg Fink: Excellent question. If a breach of unsecured protected health information affects fewer than 500 individuals, a covered entity must notify the secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. So, short answer, yes. If a practice has only that small breach, they have 60 days before the end of the year to submit it to the Office of Civil Rights.

Shanen Wright: "What's a good policy related to changing passwords? How often do you recommend that passwords get updated or changed?"

Greg Fink: The best policy is to have long, more complex passwords and change them every 90 days.

Shanen Wright: All right. We're coming to the top of the hour. I do not see any questions that we missed. So, I think we will wrap it up for this afternoon. Thanks so much, Greg, for that excellent presentation and also fielding all those questions. Obviously people do have a lot of questions around the security risk analysis and we hope that we answered a lot of your questions today. We hope you found this to be very informative and beneficial to your practice.

When you close out of today's session, you will be automatically directed to a very brief survey. We ask that you please take a moment to complete it as your feedback is very valuable to us. We did have a couple questions asking about the slide deck from today's presentation. I did email that out to everyone this morning who registered to attend the session. So, if you didn't get a chance to check your email, that may already be sitting in your inbox. But if you did not get that, we will be posting the slide deck along with the recording and the transcript of today's session on the Quality Insights website. It'll be under the Archived Events tab, which can be found under the main Events tab. I will send out an email to everybody with that link so you can access all those resources. So, thanks again so much for joining us today. We hope you have a great rest of the day, and the session is now concluded.

This material was prepared by Quality Insights, the Medicare Quality Innovation Network-Quality Improvement Organization for West Virginia, Pennsylvania, Delaware, New Jersey and Louisiana under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents presented do not necessarily reflect CMS policy. Publication number QI-D1M-100517