Elizabeth Zepko:

Hello everyone. Good afternoon to most folks, but good morning to the folks out there on the West Coast and welcome to today's webinar in the HIT Privacy and Security series, How To Prevent A Cyber Attack sponsored by the National Association of Community Health Centers. My name is Elizabeth Zepko. I'm a Program Associate in the Training and Technical Assistance Department here at NACHC, and I'm pleased to bring you this webinar along with my colleague Andy Gulati, Manager of HIT Trainings and Technical Assistance. Before we get started, I would like to make a few housekeeping announcements.

Elizabeth Zepko:

You have joined this online event by dialing in. All lines have been automatically muted. This is to avoid any background noise interference. The duration of this webinar is approximately 90 minutes including introductions, presentations, and Q&A. If you have questions throughout the webinar, feel free to pose them in the Q&A box that's located in the lower right hand side of your computer screen, so if everybody can find it. Again, it's a gray and white box, Q&A listed. Type your questions into that box at any time and hit send to all panelists. Will receive your questions. We have slots dedicated in the presentations where we'll stop and answer those questions throughout the webinar. So again, if something strikes you in the middle of one of the slides, feel free to shoot that into the Q&A box. And when we pause for questions, we'll go in order of the Q&A.

Elizabeth Zepko:

Let us remind you that today's event is being recorded and will be available on the MyNACHC Learning Center within a week. After this webinar is complete, you'll be presented with a brief survey. This survey lets us know how we did, how valuable this webinar was to you, and directly informs us of future training and technical assistance. We value your feedback and encourage you to complete the survey. At this time. I'm going to be turning things over to Andy. He'll be introducing today's speaker. Andy.

Andy Gulati:

Okay. Thank you so much Liz. Good morning everyone on the West Coast and good afternoon to those here on the East Coast. As Liz mentioned, my name is Andy Gulati and I'm the Manager for Health IT Training here at NEC. We're very pleased to bring you the second webinar today which is the second webinar on a two-part series on privacy and security. These webinars are made possible through funding from the Bureau of Primary Healthcare. Our speaker today is again Adam Bullian. Adam presented last week as well and I hope most of you on the call today will able to join last week's call if you want. The recording for last week's webinar as well as the documentation that was provided including the PowerPoint is available on the my NEC website. And as we move through today's presentation, I will post that link on the right hand side panel of your screen so you will have the link that you can go through to view last week's presentation.

Andy Gulati:

A brief introduction for Adam. Adam serves as the Director at QIP Solutions. He actively assists organizations in creating HIPAA compliance programs that meet specific needs of the organizations. Adam is also a frequent writer and present on HIPAA-related topics. He holds a bachelor's degree in history and political science from West Virginia University and a Juris Doctorate Degree from the West Virginia University College of Law. On today's webinar, Adam will be discussing the process of incident investigation, when an incident is to be classified as a breach, and what a breach response should look like. He will also cover appropriate physical, technical and administrative safeguards necessary to

protect PHI. And finally actionable steps that you at your health centers can take to secure PHI will also be covered.

Andy Gulati:

Without further ado, at this point, I'd like to handle over to Adam so he can get us going with the presentation. Adam.

Adam Bullian:

Great. Thanks Andy and thanks Liz. Uh, welcome to all of those who are joining. Good morning and good afternoon. Thanks to those, and welcome back to those that joined last week as well. If you're new this week, welcome, and we hope that you find this presentation very informative. I want to echo what was stated earlier about questions. Personally, I really appreciate questions throughout and as was mentioned, we've built in some spots along the way to address those questions, to try and do it in as orderly a fashion as possible. We'll try to get through as many as we can, while still balancing the fact that we want to get through all of the content.

Adam Bullian:

So type your questions in as we hit upon a topic that may be of interest or that you would like some additional information on. So just sort of to piggyback on what Andy said, so the agenda for this call or this webinar is we're going to talk generally about the security rule. We're going to talk about the administrative, physical and technical safeguards. But we really want to provide as much information to you as possible that you can take to your health center and implement. You should have received some resources in incident response policy and plan as well as a information system monitoring plan and a policy as well. So we're going to talk about the actionable steps, we're going to leverage some of those resources as well, and then we'll wind out by talking about incident investigation and breach response.

Adam Bullian:

Starting off generally, putting the HIPAA security rule in its proper context, it is one of technically three rules that make up HIPAA. We don't always think of HIPAA as being three separate things, but as far as the legislation and implementing regulations, that's what it is. So there was the privacy rule, which we discussed in depth last week that was passed first, and then the security rule and the breach notification rule. So today, clearly, we're focusing on the security rule. It requires covered entities i.e. community health centers and business associates to implement administrative, technical and physical safeguards for protecting PHI in electronic form. So we're not really talking about paper PHI, which is obviously becoming less and less prevalent. The security rule, for obvious reasons, focuses only on electronic PHI.

Adam Bullian:

The goal of the role is three things to ensure PHI is confidential or kept private, to ensure its integrity, that it's not altered or it's not destroyed inappropriately, and it's availability, that it's accessible, that it's usable. Those are the three things that the security rule is trying to do. And the objective also is to identify and protect against reasonably anticipated threats. At this time in the industry and in the environment that we live in from a technical standpoint, we have to think that that hacks, that inappropriate access or disclosure by the loss of a device or something of that nature is a reasonably anticipated threat. So those are the kinds of things that we are focused on.

Adam Bullian:

So there are two types of implementation specifications in this HIPAA security rule. And to some people, this creates some confusion, this means HIPAA has a lot of great in it. To other people, myself being one of them. This means that to some degree we can be creative, we can think about what is right for your specific organization. Because if you think about HIPAA, it applies to single physician practices, and it also applies to very large hospital systems and health plans. So there had to be some flexibility built in because what's possible for a single physician practice to implement and do is not the same. That is what's possible for a large health system to do. And that's why there are certain things in the security rule that are required. These things must be implemented and we're going to outline what all of those required elements in the security rule are.

Adam Bullian:

These are things like having a unique user identification. There are other things which are considered to be addressable, and these must be implemented if it's reasonable and appropriate for your organization to implement that. These are things like having automatic log off of workstations or having your electronic health record automatically log off after a period of inactivity by whoever is signed in. So the question always becomes how do you determine what is reasonable and appropriate? And these are the things that you take into consideration, the size, the complexity, and the capabilities of your organization. This is where we really get into differentiating between the large organizations and the very, very small organizations, and why on the addressable implementation specifications, it's okay for a large organization to do something and a small organization maybe to not do that. You also take into account your technical hardware and software infrastructure.

Adam Bullian:

So if it may not be something that you have the technical capabilities to do without expending a significant sum of money, then that's something that you would be taken into consideration. Also, the costs of the security measures. We'll talk about encryption in depth at some points throughout for sure, but encryption is something that certainly in recent years the cost has gone down for full disk encryption or for encrypting emails and so forth. But that's something that has always been considered. It is an addressable implementation specification. When the cost was very high, then the organizations were saying, "It's not reasonable or appropriate for me to do it because it's cost prohibitive." But you also have to balance all of these, the likelihood and the potential impact of a potential risk to the PHI. So these are the things that you have to take into consideration when you're determining which of these addressable implementation specifications are right for you.

Adam Bullian:

And the important thing to know as with anything in HIPAA is document. As you determine, or as you take something under consideration to determine is it reasonable or appropriate from what organization to implement this, let's say encryption for instance, encrypted email, then what you would want to do, regardless of what the outcome of that determination is, document. "These are the things that we took into consideration. We factored in our size, we factored in the cost of the security measure, our technical infrastructure, the likelihood of the impact. And based on that determination, this is what the determination was."

Adam Bullian:

On this slide, what I wanted to do, this is a copy of section 164.312 of HIPAA. What I wanted to do was show you in the rule that this is how the required and the addressable implementation specifications go.

So something like unique user identification, you can see in parentheses that that is identified as a required implementation specification. You must assign a unique name and/or number for identifying and tracking user identity. Alternatively, something like automatic logoff, that is as you can see, addressable. And that is to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. So for all of these things in the security role, they go through what is required, what must you do, and again, we're going to outline what all of those things are and then the things that you have to consider based on that determination or that, that those, that analysis that we outlined on the last slide and determine is it appropriate, is it reasonable for your organization to implement these things?

Adam Bullian:

There are administrative safeguards within the security role. What is an administrative safeguard? What are the administrative safeguards that we're talking about? There is security management process. This is identifying and analyzing the potential risks to your organization, implementing reasonable and appropriate security measures that reduce those risks and vulnerabilities. This is what we're talking about when we're talking about doing a security risk analysis. We're going to talk about doing a security risk analysis and all of the steps on later slides, but this is why it's important. A security risk analysis is the process and the documentation that you're going to go through to determine which of those addressable implementation specifications are reasonable and appropriate for you. So another administrative safeguard is determining the security personnel, identifying a security officer. Who is the point of contact in your organization for staff that have questions? Who is running this operation, if you will, from a HIPAA compliance perspective?

Adam Bullian:

So we have information access management that is distilled down to having safeguards that only allow the minimum amount of access to the PHI as necessary, so role-based access control. There's workforce training and management, you have to train your staff, you have to train them periodically, you have to train them on certain things. We'll talk more about that as well. And evaluation, HIPAA is something that is always in motion. A HIPAA compliance program is constantly being evaluated, determining what's right for the organization. The things that we've implemented, the safeguards that we've implemented, are they working? Are they the right things that we need to be doing? Are they still reasonable and appropriate? Okay, these are the required administrative safeguards.

Adam Bullian:

So you must conduct a security risk analysis, and from that you must implement a risk management plan. So the risk analysis will take in to consideration all of the risks and all of the things that you need to do. And that risk management plan really spells out, "Here are the things that we're going to do. We're going to implement policies and procedures. We're going to implement automatic log off. We're going to encrypt PHI." Whatever the case is. Another required administrative safeguard is to have a sanctions policy. It doesn't have to be specific to HIPAA, right? So it can be a general HR policy. But what it has to say is that for policy violations in the organization or violations of procedure, staff can be punished. They can be up to and including termination if that's appropriate. So it has to put the staff on notice that if you violate any policy, but these are specific to HIPPA, you can be punished for those.

Adam Bullian:

So another required administrative safeguard is to review your safeguards periodically. Again, this has to be something that's ongoing. Assign responsibility of the implementation of all this and the management of all this to at least one individual or one role. Sometimes it's more appropriate to have a role as opposed to an individual, as some organizations have had somewhat frequent turnover, so it's better to just say our security officer is our CEO or our CIO or our CTO or something like that. You must isolate clearinghouse functions. So what you want to do is ensure that any clearing house that you're participating in, you're seeing only the necessary information of that clearinghouse, you're not seeing all the participants' information, and that only the members and your staff that need access to that clearing house information have it.

Adam Bullian:

Implementing incident response and reporting plan, we'll talk about that later. You must implement a data backup plan. How are you backing up your data? You must have a document that talks about that. A disaster recovery plan. What happens if your health center is hit by some type of natural disaster? What happens if there's a ransomware attack and your systems are down? It's not just an environmental threat, these are also technical threats because if we remember HIPAA, the security rule is talking about availability of the information. So if your systems are down, if you're not able to pull an individual's PHI or pull the record up, then you have an availability issue.

Adam Bullian:

If that's caused by ransomware, if that's caused by some type of virus in your system that's preventing you from doing that, you need to have a disaster recovery plan in place to talk about how you're going to get these things back up and running. An emergency mode operation plan, which dovetails nicely with the disaster recovery plan. When you are in those sort of disastrous situations or emergency modes, how are you still going to provide services? How are you going to still be able to make the PHI available to individuals that need it? You need to evaluate a contingency plan and you need to execute business associate agreements.

Adam Bullian:

Okay. So that is administrative safeguards by far the largest of the three. Now we'll talk about physical safeguards. Physical safeguards boil down to the facility access, the building structure where you serve... your health center, whether it be a mobile clinic, whether it be a brick and mortar type of a building as well as workstation and device security. So facility access, who can get into restricted areas? Who has access to the server room, those types of things. Those need to be accounted for. Where are the locks? Also privacy screens and things to prevent snooping or to prevent somebody in a high traffic area being able to see somebody else's information. Workstation and device security is about proper use and access to devices with PHI on them.

Adam Bullian:

This includes transfer, so as you're moving information in and out of the facility on a device, but it also talks about end of life issues. So as you have a laptop, or a desktop computer, or a server or something for that matter that has reached its end of life, if it has PHI on it, that PHI has to be removed properly so that you can dispose of that device correctly. If you just dispose of it in the landfill, there's the potential that there's PHI on there. We're not just talking also about hitting the delete button, because anyone who knows much about IT knows that when you delete something at that level, it's not really deleted. It

can oftentimes be retrieved. So we're talking about wiping and actually completely removing the information.

Adam Bullian:

So what are the required physical safeguards? There are four. Workstation use. This is things like acceptable use. What kinds of websites can your staff not go to if you allow them to at times use a health center provided device for limited personal use? Are they allowed to use social media when they're at work? Things like that. Also, workstation security. These are things like having up-to-date patches, having up-to-date antivirus software installed on all of your devices, having the automatic timeout if it's appropriate, having a password protected cell phones if you use that or tablets, things like that. As well as device and media disposal as we talked about, making sure that you don't just discard something that all of the PHI or the potential of the PHI is on there, that the whole device has been wiped and that you make sure that no PHI still exists.

Adam Bullian:

And reuse. We're in a time where we're thinking about you may lease printers. Printers are something that are often... Most people don't realize it, but printers store some of the information that they print, specifically information that is copied, same with fax machines, and also many medical devices do the same thing. And so these are things that as you turn them in, if you lease it, if you lease these devices is you turn them back in. If there's still PHI on there, that could potentially be a breach. You may need a business associate agreement with the organization that you lease from, or you need to make sure that you wipe all of that information before you turn that back to whoever you lease it from.

Adam Bullian:

And finally we have technical safeguards. So these are things like access control. Who has access to what information? Again, we sort of think about this through the lens of the minimum necessary rule that you should only access the minimum amount of PHI necessary for anyone to do their job. And you can build in technical walls, if you will, around certain information so that people only access the information that they need. They don't even have the opportunity to go and access other information. Audit controls. One of the resources that that was sent out before today's call, is about implementing ongoing monitoring or auditing. Are you generating certain logs? You probably should be, and that resource takes you through the logs that you should consider generating. And how do you review those? Are you periodically reviewing them? Are you doing it on a consistent schedule? Are you reviewing everything or are you just reviewing a sample?

Adam Bullian:

So integrity controls, this is something to make sure that only individuals with proper authority and under the proper authority can alter any information that has already been entered. So who can go back and change a record after it's been entered? And only people who have appropriate access can destroy or delete certain information. And finally, transmission security. So much PHI is transferred through electronic channels or electronic medium, whether it be by email or you potentially have externally hosted electronic health record. PHI is being exchanged electronically from whoever's or wherever that your EHR is hosted back to your specific site, as well as internally in your organization. How are those things done? Do you have firewalls in place to prevent unauthorized access?

Adam Bullian:

What are the required technical safeguards? There are also four here. Having unique user identification. Every person in your organization who has access to PHI must have their own login. It cannot be shared logins, there should not be any type of universal login. Every member of your staff, if they access PHI, must have their own specific login. It must have an emergency access procedure. So what are you going to do in the event that your site is down, your EHR is down, how are you going to continue to make PHI available to see patients as needed? Audit controls. Reviewing those logs, looking for suspicious things, things that might raise a concern. And person or entity authentication. So authentication is about when you're connecting virtually to your electronic health record, there is an authentication that must be done so that wherever that EHR is hosted knows that whoever's trying to connect with that is an authenticated user. This could be done through different keys and things like that. And you also need to have person authentication. This is essentially having passwords, strong passwords that go along with that user identification.

Adam Bullian:

Okay, so this is our first junction right before we change topics a little bit. For any questions, I'm just going through, I don't see any questions at this time. Okay.

Elizabeth Zepko:

Adam, I don't have anything on my end and I just want to remind folks we definitely want to take advantage of Adam being here. I know that this is a very interesting topic, so maybe things are bubbling in your head of what should I ask? Everything could be answered possibly. So make sure you put your question into the Q&A box. It's located in the lower right hand side of your computer screen. All you need to do is type and hit send, and whenever we have our next question break Adam will go through them. Adam.

Adam Bullian:

Yes. Thank you. Any questions you have on any of the topics that we're covering or anything related would certainly be appropriate. So now what we're going to do is talk about six individual actionable steps. We want to talk about what are the things that you can do in your health center to really eliminate or potentially eliminate, at least decrease the risk of some type of cyber attack, some type of inappropriate access to electronic PHI? The first thing we're going to talk about is conducting a risk assessment. We're going to talk in depth about that. And then how do you take that risk assessment and put it into a plan of action. We're going to touch on policies and procedures. This is also something that we discussed for anyone that was on the webinar last week. We're going to talk about workforce training and we're going to talk about implementing audit controls and then the review and assessing and redesigning of these safeguards.

Adam Bullian:

Okay, big important topic. What is a risk assessment? There are four critical steps to conducting a thorough risk assessment. There's some things to keep in mind. First, the risk analysis must be organization-wide. It does you no good to do a limited risk analysis on just a piece of your organization, maybe one system or one location because everything is interconnected. Everything relies on something else. So what you need to do is focus on the entire organization. Other things to keep in mind is when do you need to do a risk analysis? The rule itself just says that a risk analysis must be done periodically. The best practice in the industry is to conduct one at least every two years. It's good to get in the habit of

doing one and then at least every year looking at it and making sure has anything changed? Is this still accurate? Does this still reflect the most likely risks and threats to our organization?

Adam Bullian:

Also as you have what I call big changes, big changes would be adding or closing a location. So if you add a site, if you change the physical location of your site or of your health center from one building to the next, or if you close a site, that's a big change and would really require you to look at the new risks that are associated with that, certainly as you put in new pieces of technology. If you deploy a new electronic health record, you need to do a fresh security risk analysis. Everything is changed. You don't know what the risks are. Whatever you had identified as risks before with your own EHR, throw it completely out the window because you have no idea if it's appropriate or not.

Adam Bullian:

So big changes, adding locations, closing locations or large changes of your systems, your IT systems, how you operate. Okay, what are the four steps to a risk assessment? What are we looking at? The first thing is to do an inventory of all of the PHI in your organization. Where does PHI live? Mostly electronically, but also physically, right? And this gets down to things like the device level, the application level. Do you allow staff to save PHI on their desktop? If you do, then there's likely PHI on the desktops, the computers, the workstations as well as laptops. Do you allow PHI to be emailed? If so, that's an application.

Adam Bullian:

Servers: Are the servers located on-site? Are they hosted elsewhere? What you need to know is you need to have a full view of where PHI is in your organization so that you can even begin to know what the risks are and what you need to protect. This should also include, I think it's good to include paper PHI in this. Because paper PHI hides, right? It's in a closet, it's in a filing cabinet, but we would want to make sure that those things have locks on doors, have the locked filing cabinets. That's PHI too that needs to be protected. It's lightly outside the scope of the security rule, but I think it's in the spirit of protecting all of the Phi that your organization has. So we're talking about doing a walkthrough of the organization. Where are the computers? Do those computers have access to PHI? Is the PHI saved on them? Where are the servers? And do a mapping. Here's the server room. It's room number one on the third floor. Or here's the closet. It's in room number 12. There's paper in there, and it can be done in a spreadsheet, but what you need to do is get that full scope.

Adam Bullian:

So that's step one. Step two is to do an assessment of all of the risks. This is something, it can be very helpful to have some type of tool. And in one of the later slides, just before we end, there are a couple of links to resources. And one of those is the security risk analysis tool that was put together by the office of national coordinator at the Federal Department of Health and Human Services. It's long, it's very, very thorough, but the good thing about that is that it helps you identify potential risks because otherwise you're just going to be looking around and trying to sort of brainstorm what these risks are.

Adam Bullian:

Something like that is going to provide a guide. It's going to be very helpful to narrowing your world and narrowing your focus to really think about only certain risks. There's also another resource which I'll talk about more later. It's the HIPAA collaborative of Wisconsin. If you were on last week, I also provided

that as a resource. It is a library of many, many templates that are free for you to use and customize and leverage in any way. It's a very, very, very good resource. They also have a toolkit for conducting a risk assessment or risk analysis, which focuses in on many of the same risks that we're talking about in this section. So you take a look at all of the risks. For instance, there may be in the toolkit or in the ONC risk analysis tool, something like, is PHI on laptops that leave the facility?

Adam Bullian:

That's a potential risk. So it will ask you, "Is that something you need to consider?" You will say, "Yes, we do that." Or you may say, "Well, yes, laptops are allowed to leave the facility, staff take them home, they travel with them various places. Maybe they're going from site to site, whatever the case is. But those laptops are encrypted. So first step is to identify the risk. Second step is to identify any existing safeguards that you have in place that mitigates that risk, that lessens that risk to some degree. Unfortunately it's not just good enough to sort of identify. As you're doing this very thorough risk analysis, you want to make sure that if you have identified a safeguard, go in, take the time to make sure it's properly implemented, and properly document. So do you have a policy and a procedure in place that say, "We encrypt all laptops." Or all laptops that leave the facility.

Adam Bullian:

And we have a procedure in place that talks about this is how the encryption is done, this is who's responsible for that, so forth. And you'll look to make sure so you'll see you have a document. That document is important as we will talk about more in ensuring the Prince or vacation of that safeguard into the future, and it's also outside verification and validation that you're doing that. And then you'll check and you'll make sure, "Okay, this is something that we're actually doing." Do a spot check of a couple of laptops and say, "Okay, yes, this laptop is encrypted. That laptop is encrypted." Once you take all of that information, you have the risk, you determined that there is an existing safeguard that mitigates that risk, that safeguard is documented and it's implemented.

Adam Bullian:

Now you establish a risk score, and I would encourage you, many of the tools out there do this, is to put a number on there. Set a range, right? One to nine, one to 25, whatever works for you, as long as it's consistent throughout the whole process. And say, "Okay, we identify the risk of laptops with PHI leaving the facility. That's a high risk, so that's a nine." But then we can take that down significantly because only laptops that leave the facility are encrypted and we verify that there's a policy in place and that it's properly implemented. So we're going to take that nine, and move that down to a three. We've quantifiably mitigated that risk.

Adam Bullian:

So now you have a score of a nine or a three or whatever it is, a 15, however your scale is, and then you're going to establish a likelihood. So the likelihood of this happening, of this risk causing a breach or an inappropriate access or disclosure of PHI is also three, or it's nine because I don't have any mitigating safeguards. So then you put those together and now you have a risk score. When you quantify it, when you put numbers around these things, it helps you to identify in the end, these are the most critical things that I need to work on. And as we talk about the output of the risk analysis, that's going to be creating that prioritized plan of activities that you need to do.

Adam Bullian:

Okay. So step one of a risk analysis is the inventory. Step two is the risk assessment, the assessment of all of the risks in your organization. Step three is to do a threat assessment. We think about threats in the terms of environmental, human malicious and human accidental. And these can just be factored on a likelihood scale. So environmental risks; earthquakes. An earthquake in Southern California for a health center in Southern California may be occasional to rare, whereas an earthquake in my home state of West Virginia is rare to never. So you're going to just factor these threats in, as well as accidental human threats, right? So the threat of the loss of a laptop, that's an accidental threat. No one intends frequently to lose a laptop. But that could be rare or never if you have a policy in place that forbids laptops from leaving the facility.

Adam Bullian:

So you're going to factor in all of these threats as well. And you can put these on a never, rare, occasional or frequent factor. You can also put some numbers around there. But as long as you're factoring in, well this is how frequently they potentially happen. And then finally, the last step is to do a technical vulnerability scan of your systems. This is best done by a independent third party. So if you have an MSP or somebody that's working with you to manage your EHR or host your EHR and they also do scans, I would encourage you to try and find somebody independent of them, to do just a scan. You want to do a passive and active and an asset scan of the entire network. It's important that it be the entire network.

Adam Bullian:

And what that's going to do is that's going to help you identify technical vulnerabilities. These are things that are not easy to identify in policies and procedures. You may have a policy that says we have up-to-date and current antivirus software, or we keep all of our patches up to date. But a technical vulnerability scan is actually going to scan your system and give you a report that says you have Adobe patches that are out of date. You have out of date Java patches, you're using outdated encryption technology. So these are things that really are very valuable from a technical perspective.

Adam Bullian:

The last thing as you take all of these four items together is to put them into a report. And I want to encourage you that as long as you think about this objectively, this report doesn't have to be outsourced to a consultant or to another organization. As I've mentioned, there are resources to help you do it, but it doesn't do you any good to sugarcoat things or to put inaccurate positive spin. What you need to do is be serious and very honest about the risks to your organization. But you can put this report together yourself. It doesn't have to be fancy, it doesn't have to have graphics or anything like that. But outline what methodology was used. We did a scan, we did an inventory, we did a threat assessment, we did a risk assessment. Talk a little bit about that so that anyone that's coming in can say, "Oh yeah, they factored in all of these pieces." This is an organization-wide risk analysis. This is what we need to see.

Adam Bullian:

And then it's going to identify findings. These are the risks that we identified, these are the risks that are mitigated, these are the risks that are unmitigated or that need to be mitigated. And then very important, is here are the steps that we need to take. Here are the risks that we need to remediate. Here are the things that we're going to do to fix these areas. And that's a risk analysis. It should be a very thorough process, it should be something that again, takes in the whole organization, it's organization-

wide, and it should be something that's done periodically. But what it gives you at the end is an opportunity to prioritize remediation.

Adam Bullian:

Again, we've tried to put a quantity, we try to quantify the risks in some function, right? And now you're going to determine, "Here are the things that I need to do." And you want to take into account what are the greatest risks to your organization? Based on how you operate, how are you doing business? How are you exchanging information? How is your staff accessing information? It's very specific. The likelihood and the impact that these risks cause. You're also going to take in the size of your organization the resources that may be necessary. This is resources in a general sense, personnel resources as well as resources that are out of pocket expenditures and your complexity and then the cost, right? So what is it going to take from a time, financial and other resources perspective to remediate these activities? And again, you may determine if it's something that is an addressable safeguard, that it's too expensive for you to do. That's okay, as long as you've taken into consideration, "Here's the risk, here's the likelihood, here's what it's going to cost me." It's too resource intensive.

Adam Bullian:

Once you do all that, what you will get is a specific order of steps that need to be taken. First thing we're going to do is our patches are out of date. That's the risk. So we're going to implement a patch management operation in which we fix all the patches that are outstanding. And every month we do a check to make sure that all the new patches that are necessary have been applied. Something like that. And document. Document, document, document. What was the final remediation plan? And then put those points along the way so that you're saying, "Okay, we said every month we're going to check for updated patches and make sure that everything has been applied." So at month two, have a spreadsheet that says, "We checked for these patches, we found two missing, we applied that. Month three, we did a check for the patches on February 3rd and all patches were up to date." Now you've identified the risk, you took the initial remediation step to fix it, and you put that longterm plan in place to keep those risks low.

Adam Bullian:

Okay. So I'm going to stop here. I'll take some questions. Someone asked the meaningful use requirements of SRA. One of the things when you attest to meaningful use is you're attesting to completing a security risk analysis annually. So if you attested to meaningful use, you're saying to the regulators, to the potential auditors that I have a risk assessment in place, that it takes in everything in my organization and that I'm remediating the risks that I identify. If you attested and you don't have a risk analysis in place, or it's now outdated, then you are essentially in violation of that attestation. You're in some respects breaching that contract that you signed in order to accept the meaningful use incentive.

Adam Bullian:

And there are some organizations that are running into some troubles because there was a financial outlay for the government. They are doing periodic audits. They're asking for the risk analysis report. So when I say that report is very important, what that report could potentially serve is as the validation to those auditors that, "Yes, I did the risk analysis. I did it on this date and here's the process of the steps that I've taken since then to remediate those issues."

Adam Bullian:

Next question is what's the HIPAA rule for sending faxes inter office from site to site within your company? So HIPAA doesn't speak specifically on faxes, it doesn't speak specifically about email, it doesn't speak specifically about any sort of specific type of electronic transfer of PHI. What HIPAA says generally is that number one, that transfer needs to be secure. It doesn't mean you have to have an encrypted fax line or something like that. You're certainly permitted to send those faxes from site to site within your company. What you would want to do is number one, confirm that you have the proper recipient. One of the most common incidences we'll talk about more that I see in my work is people that have faxed or emailed PHI to the wrong recipient. So the more that you can ensure that you have the right person, the better.

Adam Bullian:

If you can encrypt that in transmission, that's good. You don't have to get the patient to consent or to authorize that transfer as we talked about last week, and if you have specific questions or concerns about authorizations and consents, I would encourage you and anyone that wasn't on last week to go back and listen to that recording. But this is something that is a permitted disclosure for treatment most likely or payments or healthcare operations. So it's not something that the patient has to consent to that so you're fine and actually doing it. The other thing is to consider the end of life of those fax machines.

Adam Bullian:

So again, are you leasing it? If you lease it before you send it back to the leasing company, make sure that the PHI is removed or that that company is going to remove it. If the leasing company is going to remove it for you, make sure that you have a business associate agreement with them because physically when you hand them that fax machine, there is likely PHI stored on there and you are disclosing PHI to them by handing them that fax machine. So you have to have a business associate agreement with them if they're going to do the proper removal of PHI on that machine.

Adam Bullian:

Okay. Next question. And if I didn't quite answer that question on faxes, please type in something else and I'll try to be a little bit more elaborate. Next question. If we have dedicated IT consultant who manages our network, do you think we should use the same company to conduct the scan or use a different company? I would use a different company. When you're doing the security risk assessment, specifically when you're doing a scan, you want some independence there. You don't want the company that manages the network to also be the company that scans. There's a little bit of a conflict of interest. They may not be as honest with themselves or as honest with you about the risks. You never know. I'm sure 99% of the companies out there are honest and they're interested in protecting you. But I would prefer to have fresh eyes and somebody who is not involved in the maintenance or the design of that network assessing with almost anything else. I would encourage you to to use a different company for that.

Adam Bullian:

Someone asked me what encryption software I would recommend. I don't have a specific company that I've worked with. A lot of the community health centers that I work with use many different things. And it also depends on whether you're talking about full disk encryption on a device like a laptop or a tablet, or you're talking about encrypted transfer, like encrypting an email. Because so much of it just depends on your organization. When we're talking about email encryption, oftentimes there are two types of

email encryption. There are the types that scan the email for anything that's potentially personally identifiable, a phone number or a string of numbers that looks like a phone number, or looks like a medical record number, or looks like the social security number or credit card number or a full name or date of birth.

Adam Bullian:

And then they will encrypt that email if they detect a potential of PHI or anything really personally identifiable in that. There are pluses and minuses to that. Plus are you don't have to train your staff as much to do much because it's pretty automatic, but you're going to get a lot of over encryption. Alternatively, you may have encrypted email where you have to push a button in the composition of the email or type encrypted in the subject line or encrypt in the subject line. So in that you really have to think about you're going to have to train your staff more, identify what types of emails we need to be encrypted and things like that. So I would encourage you, there are lots of good companies out there. The community health centers that I'm working with, many of them are moving to some type of encryption, so the price point is moving in our direction.

Adam Bullian:

A few years ago it was still very expensive, but it's moving in the right direction for us for sure. ut it is going to take a little bit of research on your part. And second question, can you set a password-protected document containing PHI as an email attachment? Yes. Assuming you're sending it for a permitted or required reason, then yes. You're sending it to somebody who has a right to know that or has the proper access to have that PHI. Sending it as a password-protected email attachment is certainly good and certainly something that you can do.

Adam Bullian:

My other recommendation is be sure that you don't send a password in the same email as the password-protected attachment because if somebody has access to that one email, now they have all of the keys to the kingdom. So usually when we're talking about encryption or password-protected attachments, it's best to send the email with the protected attachment, and then call the recipient or text the recipient, use some other form of communication so that it's nearly impossible for somebody who may have gained access to their email exclusively to get access to that information.

Adam Bullian:

Another question was, after the report is finished, how would a health center prioritize the risks for remediation? Hopefully we covered that a little bit in this slide. What you want to do is hopefully you're going through and quantifying these things by risk. You're not encrypting laptops, but laptops have PHI on them and they're removed from the facility on a consistent basis. Um, that's something that would be a high risk, a nine, a 20, whatever your scale is. And you can use any scale that fancy that would be fine. And then you know you're taking risks down by certain magnitude as you identify the proper implementation and documentation of mitigating safeguards, what you're going to then do is you're going to have a list of things.

Adam Bullian:

And these are going to be nine risks and seven risks and things with a nine risk score, I should say, or a seven risk score. And that's going to give you an indication of, "Oh, I need to do that. That nine is a very high risk. So I'm going to prioritize that first." And then what you factor in is we talked about here is, are

these things cost prohibitive? Are they technology prohibitive? And if they are, you would say, "Hey, that nine risk, that is developing a contingency plan, which is a six-month project. We are just right now in the middle of our UDS reporting, so I can't get to this until March 15th. So I'm going to move that down the list. I'm going to start it on March 15th or something like that." You have a target date for starting it. So you still have a plan. It's just maybe not the first thing that you're going to do.

Adam Bullian:

So next question. Could any IT company do the risk assessment document, or does it have to be a specific risk assessment document? Any IT company that again has some independence from the day-to-day operations, I would say, can really do this assuming they have capabilities to do the scan and they're thorough. You want to make sure that they understand what are the requirements... your specific requirements of HIPAA, that there are some things that you must do. There are other things that you have some flexibility, the addressable requirements. But there's no specific format that's outlined in as to what the document looks like. As I mentioned, it's good to explain your methodology so that if you ever get an auditor who comes potentially for meaningful use, or if we see another round of HIPAA audits, they can see this is how we did the risk assessment, these are the things that we took into consideration. And then identify what the risks are and explain, the important thing is to explain your thought process.

Adam Bullian:

Explain that, "Yes, we identified this is a risk, but we have these mitigating safeguards and that's why it's not a high risk." So it's not spelled out perfectly or in any level of detail in the rule what these things have to look like. So I would say any reputable IT company could put this document together for you.

Adam Bullian:

Last question before we move on to the next section. Again, I appreciate these questions very much. If you have competing risks, are there certain risks that should be prioritized first? Again, I would prioritize your higher risks. First, anything that's really posing an immediate potential threat to the organization, I would cover that first. And then if you do this scoring and you have let's say three or four that you've identified as a nine risk score or whatever scale you use as your highest, then you get into some of these other things like the time it's going to take to remediate the costs, opportunity costs if you will, that may be associated. And hopefully what you can do is say, "This one is a high risk, it's going to be easier for me to remediate. So I'm going to go ahead and do that one first." So there's some element of getting to the low hanging fruit, to really help remediate those risks.

Adam Bullian:

Okay. So this is a duplicate slide from the presentation last week. So hopefully not to dwell too long for those that are joining both of these sessions, but it's on policies and procedures as we talked about through the risk analysis, and as we talked about many of the required safeguards physical, technical and administrative, there are a lot of things that must be documented and tracked, and those are done primarily through the policies and the procedures. It's really the how-to of how your organization does things and where your organization stands on certain issues related to security as well as privacy. It's going to outline what safeguards you have implemented, encryption, automatic log off, unique IDs, strong passwords, things like that. And it should be available to all of the stakeholders. So these things for the most part should be if there's something that impacts the entire staff, like a password policy or a training policy, it should be available for review to the whole staff,

Adam Bullian:

And hopefully you have some document management system that you use, where staff can look and say, "This is our policy on acceptable use. These are how I am allowed to use the electronic devices that my health center that I'm working for provides to me. I am allowed to check my personal email, but I'm not allowed to do business for anything other than the work that I'm doing for the health center." Something like that. And also something as we're going to talk more and more about as we continue through the presentation, these should be periodically reviewed and updated. If it's something that's a new policy or a new procedure, I would recommend taking a look maybe after the first month or the first 60 or 90 days of implementation just to give a check of is this working? Is it in place?

Adam Bullian:

Once it's something that's sort of been validated as running pretty smoothly and achieving the goals that were intended, then you can back the review off to maybe every six months if it's something that could be in high fluctuation, or maybe a review every 12 months. The idea is to look at it, to validate that it's still appropriate for you, that it's still working for you and do that check. These things don't have to be scrapped and redrafted every single year, but they should be read, they should be updated as needed. Many of you in your health centers, they will have to go through a board of governors' approval process if they're specifically for the policies of your organization. And they may have to go through a governance committee, so it can be very cumbersome for you to do really frequent updates to these things. But I think for the most part, policies should be looked at once they're sort of rolling smoothly at least once a year.

Adam Bullian:

And finally identify one person as we talked about, identify one person who is the owner. This person is responsible for doing those updates periodically as well as implementing these things, and the initial design of that as well. And you want somebody who's very close to the process. You don't necessarily want an outsider from this specific area to come in and be responsible for the review of the implementation of these policies and thus the safeguards. The policies and the procedures are the documentation of all of the things that you do to protect the information. And when we talk about HIPAA, so much of HIPAA compliance is that documentation, this documentation to show that this is how we do things. Because no one's going to come in to verify your HIPAA compliance or to look at it and walk around your organization for six weeks to see how you actually do things. What they want to see are the policies that are there, the procedures that implement those policies, and the laws that verifies that those procedures are being implemented.

Adam Bullian:

Training. Training to me is really one of the most important things that a health center can do to secure information. We hear a lot about a brand somewhere. We hear about large data breaches. Um, what happens is that the real cause, the fundamental cause of those data breaches are human related. Not malicious human related, typically they're accidents. Somebody opens an attachment in an email. That was a really good fake on what otherwise appeared to be a legitimate email. And that attachment, it puts a virus on the system. That virus is then used to shut the system down, encrypt all the information and now somebody wants a ransom to unlock or decrypt the information. And it was maybe one employee who was going about their job, has no malicious intent at all, but they just weren't aware of what to look for and to notice that some of these emails may include suspicious or fraudulent attachments.

Adam Bullian:

The same thing, we see so many lost devices that have PHI on them. That's a potential argument for encrypting the information. But also it's something that could be... Training staff to understand, "I don't take my laptop with me and leave it on my front seat." That's a target for a potential theft. I put that laptop or I put that tablet in the truck. I put it out of sight. If I'm traveling on an airplane, I keep that with me all the time. As opposed to somebody picking up my briefcase that looks a lot like theirs. They're not trying to steal my briefcase, but they happen to pick up the wrong one and now we have a breach. No one intended anything, but the information is out of your control and you have to assess what's happening.

Adam Bullian:

So the who, the when and the how of training. Who should be trained? You should train your entire workforce. This is not just your staff, these are your volunteers, these are any contractors. Anyone that you or your organization has the primary day to day control over their functions. Those people are who you need to train. When do you need to train them? At minimum, you need to train them when they are hired. You've got to educate them, "This is how we do business. These are the safeguards that we have in place." As well as once annually, at least once annually. So you have to do the big HIPAA training where people come in and they watch a video or they hear a speaker or something like that.

Adam Bullian:

Best practice. What I encourage people to do is do some periodic trainings. It doesn't have to be formal. It can be a poster. It can be an email that goes out and says "We've identified this vulnerability, or also we have a reminder, we have a policy that says you are not to store any patient information on the desktop. It should only be stored in the electronic health records or some other secure storage area." And that email, that reminder is a way to trade. So the important thing is as you identify where procedures or policies are not being followed, take that as an opportunity to "retrain" the staff. That can be pulling everyone into a meeting, that's not very efficient and doesn't really help you see patients as frequently and as efficiently as you want. But sending an email is something that's possible.

Adam Bullian:

How? There are many, many ways. There are many good trainings out there. You can do video-based training as I mentioned, emails and posters or in-person training. You can hire somebody. I've done a virtual and in-person training for community health centers to come in. What I think in my personal opinion, and you're not going to see this written in any of the rules, but in my experience, the best way to do training is to have the stakeholders of that policy, the person who's responsible for the design and the implementation of that policy and procedure on your staff, your champion for that, to present a piece of training on that one specific topic or those several topics that they are the champion for. They can talk about, "This is our policy. This is how we implement that policy, and this is what we need you to do as an integral member of the staff."

Adam Bullian:

What's most important when you talk about training is make the training customized to your organization. I see very little value in broad trainings, canned videos or slide decks or whatever you may be able to acquire that just say something to the effect of, "You have to have a strong password." Or, "You have to have a unique user ID." Well, we encrypt emails that have PHI on them. What you want to do is make that as specific as possible because you're talking to the people that are on the ground

actually implementing these safeguards for you. So if your policy is to have a strong password, tell them how strong that password needs to be. It has to be eight alphanumeric characters, it has to have special characters, upper and lower case, and it must be changed every 90 days.

Adam Bullian:

Now you're taking your password policy and you're training them on that. Again, when it comes to encrypted email, how are you encrypting that email? Somebody has to type encrypt, "Okay, this is how you do it. This is where you type encrypt and these are the types of emails that need to be encrypted." You're not going to get that level of detail in a video because no one's going to be able to create a general video that's going to be able to get to that level of customization. You can have the videos to talk at high level, but at some point you want to get into the weeds and be very specific so that you can help staff know what they need to do.

Adam Bullian:

Audit controls is the next topic. It's the best way, and in many aspects, the only way to really determine if your safeguards are implemented properly and for detecting certain types of incidents. So you want to establish a consistent time for review, just like the policies, at the very early implementation stages you want to do a pretty frequent review. And then as things become a little bit more implemented and are rowing a little more smoothly, you can back that off a little bit, once you identify what you're looking at. Also some of these logs that we're going to be reviewing with the audit controls couldn't be very significant. They can be extensive, and you may not have the time or the resources to have somebody sit down and review the whole law. So what you can do is do a sample of those. It doesn't have to be a complete review, but you can do a limited sample but do it at higher frequency.

Adam Bullian:

So what are we talking about? What are these logs? So an access audit. So you print the log of all the individuals in your organization that has access to PHI. You're looking for things like terminated employees. Do they still have access? You're looking for people that may have changed roles and now their role-based access control is different. Is the role based access control, has it been updated? The larger logs that you would be auditing could be successful or unsuccessful login attempts. This is going to give you a good idea if you're having outside brute force attempted hacks, and may potentially identify some vulnerabilities that you have. And administrative audit, this is something that could be done with less frequency, with the assumption that you don't have that many administrators.

Adam Bullian:

But who has administrative access? Of course, that's something that should be very, very limited. But making sure that anyone who does not absolutely need administrative access doesn't have it. And looking, what changes are they making? Okay, so again, we want to make this an ongoing process. So again, set a schedule for the review of those policies, reviewing the logs, reviewing the security risk analysis. We talked a little bit already about when the security risk analysis needs to be updated, when you open and close locations, when you deploy a new EHR. Also, what I didn't mention earlier is if a breach happens, if you have something, and we'll talk more about breaches in a minute, but if you have an incident, a risk or vulnerability has been exploited. So now you want to take the opportunity to look at the whole organization. Are there other risks out there that you haven't identified?

Adam Bullian:

And again, documentation is so important in this whole process. So as you review those documents, as you review the logs, as you review the policies, note when that review was done. So your policy will say, February 3rd, 2017, it was initially implemented. July 3rd, 2017, it was reviewed, no changes or changes generally made to these sections. So you're documenting the review. Okay. Let's see if we have any questions. I'm not seeing any additional questions. We have about 10 more minutes, so we'll hopefully finish right on time and we'll talk about incident and breach response pretty quickly. So if you have any questions before we wind up in the last 10 minutes, please get those in. It can be on anything that we've covered or even potentially anything that hasn't been covered today that you just have a general question about on the overall topic of HIPAA.

Adam Bullian:

So incidents and breaches are different. We tend to hear them talked about in the same context, but they're actually different things. And incident comes first. An incident is where you are looking, you've been alerted to the potential that something inappropriate access-wise or disclosure-wise has happened, and you have to determine did it happen, was it appropriate or inappropriate? And then you're going to determine whether it was a breach. You need to have an incident response plan. And one of the resources that was included with this that I believe Andy sent out before the webinar is an incident response plan. And all of these things that we're going to talk about are included in there. So I encourage you to look at that, to use that. If you have an incident response plan in place within your health center, verify that it includes all of these things. You want to identify a team, an incident response team. Who's responsible for what? When you have an incident, if it's a small incident, it may not be as chaotic, but large incidents, hacks or loss of a device, these are incredibly chaotic times, and timing is very, very important.

Adam Bullian:

You need to have a team of people who know what they need to do, what they're responsible for. Your plan needs to determine how incidents will be investigated. If you need to include an incident alert form so that you are consistently tracking the alert of all the incidents, whether that alert came from a review of a log, whether it came from a staff member saying, "I think I have a virus." Or, "I think I downloaded something inappropriately." Or whether it came from a patient or a partner who says, "Hey, I saw my information that only you have access to on a website somewhere. What happened?" But you need to have an incident alert form included in the resources, so that you consistently track all of these things. And you need to have a specific process for what steps will be followed.

Adam Bullian:

The more you plan for it ahead of time, the easier it will be when you actually need to implement this. You'll want to have a classification for the incidents; critical, important, non-critical or non incident, so that you know, okay, this is an all hands on deck situation. This is something that could potentially take your organization offline for some time. This is important. We're still going to be able to maintain business operations, but it's important because maybe it affects a large number of people. Or something that's non-critical, it's limited, it doesn't affect the general operations. And put some specificity around what is a critical event? What is an important event? And determine the necessary steps for what happens when you determine that an incident, yes, actually is a breach. And this talks about notification to the individual, notification to a authorities at the federal level and potentially at your state level.

Adam Bullian:

So you're doing the incident investigation, you may do forensic analysis if it's a technology issue or a potential breach. You may be doing interviews with staff to determine what happened. You're gathering as much information as possible. Now you have to determine is this incident a breach? And there are four things you take into consideration. First, the nature and the extent of the PHI involved. What kind of identifiers and and how likely is it that they have been re-identified. So for instance, if you have a breach of information that contains a unique visit code or code that is generated uniquely for each individual, for each time they visit your health center. That may be hard to re-identify, it may be easy to re-identify, you never know. That must be something that you would have to take into consideration.

Adam Bullian:

Factor that in versus social security number, or full first and last name. Now we're talking about very identifiable things that don't need to be re-identified at all, they are specifically identifiable. The unauthorized person to whom the disclosure was made. This is something that oftentimes we don't know. When we fax PHI to the wrong recipient, we may know. We may get a call and they say, "Hey, you sent me this information, I'm not the intended recipient. It may be the last person that you sent a fax to, or maybe you just dialed in the wrong number." So in those instances you may know who it was disclosed to, but in other instances in the event of a loss or a theft of a device, in the event of a hack or something like that, you may not know.

Adam Bullian:

And if you don't know, you can't say that it wasn't a breach. It's hard to say. Also the same with whether the PHI was actually viewed or acquired. Depending on what kind of logs and forensic analysis you can do, you may be able to say if it was actually viewed or acquired, but if you can't, you may have to assume that it was. And the extent that the risk has been mitigated. And the thing is, if you can determine through this analysis that there's a low probability that PHI was compromised, then it's not a breach, but it has to be a low probability that Phi was compromised. Some of these things that may be hard to know, would have to be things that are actually you need to know. Otherwise it is a breach.

Adam Bullian:

I'll go through these pretty quickly because we're running out of time. If a breach occurs, you need to mitigate, you need to stop the breach. You need to do your best to determine who was affected. If you can't determine specifically who was affected, you may have to do a wide notification, because you've got to include all the potentials if you can't exclude anyone or you can't exclude all the people. And you're going to need to make notification to the individual. Under federal law, that's within 60 days of discovery, at least within 60 days. It's without unreasonable delay, but no longer than 60 days. Some states, that time is shorter. So there's some state-specific elements to that. To the department of health and human services, to the media in some instances, and to potentially state officials, likely maybe your State Attorney General.

Adam Bullian:

Again, when the breach is over, you want to identify what happened, what went right, what went wrong, what are additional risks that we may have overlooked? Do a new risk analysis. Also evaluate your response. Okay, so I'll leave this slide here. These are the resources. The first one is the general overview from Office For Civil Rights of the Security Rule. Second is the HHS' risk assessment tool that I mentioned. Third is the HIPAA Collaborative of Wisconsin or HIPAA COW. You may know it as that. Funny name, but a great resource. Their policies and procedures library, template library and then a

privacy and security blog that I write every week. Okay. So I'll jump through some of the questions. What does an SRA stand for? SRA is a security risk analysis.

Adam Bullian:

Do we have an opinion on the following scenario? An employee leaves the facility, takes a patient list with them for recruitment of patients to the new facility where he is employed. That employee when they leave your facility no longer needs access to that patient list. The patient list likely contains names, that is inappropriate access to PHI. You would need to investigate to determine what are they using it for? An individual has to specifically consent to marketing, so if they're trying to recruit patients to their new practice, they may be doing that without the appropriate authorizations.

Adam Bullian:

And the last question, I think, should we create a policy for third party support to remote in. Yes. So you should, you should have a policy and a procedure in place for any remote access to your network. So anyone who's promoting it, even if it's an employee who may be working from home, you should have a policy and a procedure for how they are authenticated, how that remote access is secure. Okay. I think that's all of the questions that we've received. I will turn it back over to Liz or Andy for any closing remarks. And just to say, my contact information is on the last slide. If you have questions going forward, feel free to reach out.

Elizabeth Zepko:

Folks, I want to thank you guys so much for joining us. Thank you, Adam. For the past two weeks it's been amazing, these webinars. Again folks, both sessions are being recorded. I believe the first one is already on my NEC. The second one, today's session should be on my NEC within the next week. Also I want to remind you, please, if you wouldn't mind filling out the brief survey once you close out of WebEx today, this information that we're using is going to help us plan some future regional trainings out in the field, so face-to-face trainings as well as some webinars in the future. So if you wouldn't mind just taking five minutes of your time to fill that up, we'd greatly appreciate it. With that, we hope that you have a great weekend and a great day at your health center. We'll see you next time. Thanks.

Adam Bullian:

Thank you everyone.

Elizabeth Zepko:

Bye everyone.