Elizabeth Zepko:

Good morning to our folks on the West Coast, and good afternoon to everybody else. Hello, and welcome to today's webinar, Privacy and Security: What You Need to Know, sponsored by the National Association of Community Health Centers. My name is Elizabeth Zepko. I'm a program associate in the Training and Technical Business department here at NACHC, and I'm pleased to bring you this webinar along with my colleague Andy Gulati, manager of HIT training and technical assistance.

Elizabeth Zepko:

Before we get started I would like to make a few housekeeping announcements. 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 for some reason you do have a question throughout the webinar we'd like that you ask the Q&A box. It's located in the lower right hand side of your computer screen, and I do also have a visual on Webex right now, so if everybody could just take a moment to look at the Q&A.

Elizabeth Zepko:

And we will be taking questions throughout the webinar. Please keep this in mind. So whenever you have a question or a thought feel free to just enter that in the Q&A box, and we'll pause periodically to answer those questions. Make sure you hit send to all panelists, and again, I will be reading these questions out to our panelists today. If for some reason we cannot get to your questions in the time allotted we will make an attempt after the webinar is complete.

Elizabeth Zepko:

Let us remind you that today's event is being recorded, and will be available in about two weeks are our My NACHC Learning Center. After the webinar's complete you'll also be presented with a brief survey. This survey lets us know how we did, how valuable this webinar was to you, and directly inform of us future training and technical assistance. We value your feedback and encourage you to complete this survey.

Elizabeth Zepko:

Everybody should've received the log in information as you're logged into Webex right now, and attached was a slide deck, a PDF slide deck of today's presentations for you to take notes. If for some reason you do not have access to those slides because you can't find them in your email feel free to look on the right hand side of your computer screen. Right above the Q&A box you'll see a chat box. I just attached a link to Dropbox which will give you access to those PowerPoint slides that you can pull up, and download and take your notes.

Elizabeth Zepko:

At this time I'd like to turn things over to Andy, who will introducing today's presenter. Andy.

Andy Gulati:

Great. Thank you so much, Liz. Good morning everyone, and good afternoon to those on the East Coast. Thank you for joining the webinar today. My name is Andy Gulati, and like Liz said I am the manager for health information technology training here at NACHC. We are very pleased to bring you this two part

web series on privacy and security, and this was made possible through funding from HRSA, especially the Bureau of Primary Healthcare.

Andy Gulati:

Our speaker for today's webinar, and in fact for the webinar next week also, is Adam Bullian. Adam serves as the director at QIP Solutions. He actively assists organizations in creating HIPAA compliance programs that meet the specific needs of the organization. Adam is also a frequent writer and presenter on HIPAA related topics. He holds a bachelor's degree in history and political science from West Virginia University, and also drew his doctorate degree from the West Virginia University College of Law.

Andy Gulati:

On this first webinar today Adam will discuss the implementation of the HIPAA privacy rule at federally qualified health centers. He will focus on areas of HIPAA privacy including creating effective and appropriate notices of privacy practices, drafting business associate agreements, and managing business associates, proper disclosure of PHI to the patient and others, as well as necessary policies and procedures to implement.

Andy Gulati:

Before I hand over to Adam I just want to reiterate what Liz just mentioned. If you do not have the PDF or the PowerPoint deck Liz has posted that link on the right hand side chat panel. Feel free to click on that link and that should also allow you to have access to the slide deck.

Andy Gulati:

So without further ado at this point I'd like to turn over the webinar to Adam so we can get started. Adam.

Adam Bullian:

Great. Thanks Andy. Thanks Liz. I appreciate everyone joining today. As Liz mentioned I do want to reiterate that it's always great if you put any questions in that you have during the course of the presentation, that way we can address them while we're still on topic. We'll also reserve some time at the end. I certainly understand that some things may come to you later in the form of a question, and we'll definitely have some time at the end to address everything that may be left over.

Adam Bullian:

So as Andy mentioned we're going to focus today on the privacy rule in HIPAA. Next week, we'll focus primarily on security at federally qualified health centers, and community health centers. But today, we're going to talk briefly about PHI just so we're all on the same page, what is it, how do you identify what it is in your health center. We will talk about notice of privacy practices. We'll talk about the three types of disclosures, required, permitted, and authorized.

Adam Bullian:

We're also going to talk about some of the patients rights, specifically access, amendment, and the right to an accounting. We'll talk about business associates, business associate agreements, and how you at a community health center can best interface with your business associates while keeping the information that they have access to secure and private.

Adam Bullian:

Finally, we'll wind out with a discussion on policies and procedures, how to actually go about developing good policies and procedures, and why they are important, and some ideas of what some essential policies and procedures you should have at your health center.

Adam Bullian:

Focusing on specifically the privacy rule. So when we talk about HIPAA, HIPAA is really three distinct rules. There's the HIPAA privacy rule, this was the original HIPAA. It came about in 1996, and as we will discuss today focuses not just on keeping information private, and only allowing those who need and should have access to it, but also focuses on what are the patients rights when it comes to their PHI, what can you do with it, what can they allow you to do with it.

Adam Bullian:

It talks about what kinds of safeguards are really appropriate in keeping that patient information private. It sets limits on various disclosures. It limits what you can do. One of the things that I see a lot in my work with community health centers, and this is certainly understandable, is they take a very, very narrow view of the privacy rule, because they don't want to get in trouble, they don't want to disclose something that they otherwise shouldn't, so in many ways they limit a lot of the disclosures that are otherwise permitted. So we're going to talk about those and try to clarify some of the things that you're very much allowed to do.

Adam Bullian:

And also, the privacy rule also specifies what rights the patients have when it comes to their access and accounting, and various disclosures, and it's important to keep in mind while the security rule is exclusively focused on electronic PHI, think about what's in the electronic health record, the privacy rule applies to PHI in any form whether that be in paper form, in the electronic form, as well as spoken, or oral form. So we're taking a very broad approach, and the privacy rule takes a very broad approach when it defines PHI, and what protections are necessary.

Adam Bullian:

So we touched on this term already, protected health information most often can be called PHI. What is it? So it is personally identifiable information that is something that contains one of 18 identifiers which we outline in the next slide. And that information has to relate to an individual's past, present, or future physical or mental health condition, the provision of the healthcare to that individual, or the past, present, or future payment for the provision of healthcare.

Adam Bullian:

And when we get right down to it, it's really any information that is personally identifiable that relates to the delivery or payment of healthcare. I know for a fact that's most of the information that you have at community health centers. So we're talking about pretty much any patient information that you have is also protected health information.

Adam Bullian:

As we mentioned earlier there are 18 things that make something personally identifiable. One of these things on a document, a paper document, one of these things in the electronic medical record would

make that information PHI. These are things like the name, which we certainly would anticipate, but also things less anticipated, such as the address, that is anything more specific than the state. So if you have a document that talks about the provision of past, present, or future healthcare that has a ZIP code, or street address, or even a city that is PHI, as well as any elements of dates except for a year, so anything that is a month and a year that makes something PHI.

Adam Bullian:

We have some other things that we would certainly consider, telephone numbers, fax numbers, an email address, certainly a social security number. Often times I receive questions about a medical record number. A medical record number does make something PHI. It is a PHI identifier because that medical record number links back to one specific individual.

Adam Bullian:

Certainly other things, various account numbers, a certificate, or a license number, vehicle serial number, web URL, an IP address, as well as images, certainly thinking about a full face image absolutely would be personally identifiable. And then, there's always this catch all at the end that is anything that could uniquely identify the individual. So if you're not sure whether something is PHI you can come to this list and see is one of these pieces on there, if it is, it is PHI. Otherwise, you can ask yourself is it possible to identify a specific individual from the information in this documents, or on this form, whatever the case may be. If the answer to that is yes then assume it's PHI and is thus protected by HIPAA.

Adam Bullian:

So we'll switch gears now away from the broad conversation of what's PHI. Hopefully, everyone has a strong understanding of that, and we'll focus specifically on notice of privacy practices. This is one of the fundamental things in the privacy rule. One of the things that pretty much everyone in the industry is familiar with. Patients know it's most likely as that form that they fill out that they most don't read. Some certainly do read them and they should. And certainly most providers, community health centers, and otherwise are familiar with notice of privacy practices.

Adam Bullian:

But what really is a notice of privacy practice? It describes by rule, it must describe the way in which you use or disclose the patient's PHI. It also must state your duty to protect the privacy, and that's to say we will protect the privacy of the information that we generate, the information that you give us. It must say that you will provide a notice of privacy practices and you will abide by the terms of that notice. As a community health center you can think of it in many ways, and in many ways it is, a contract between your organization and the patient to say that we are going to protect the privacy of this information, and the patient signs that.

Adam Bullian:

It also describes the patient's rights and that includes the right for them to raise a complaint to you, or the secretary of health and human services, if they think their rights have been violated. It must provide a point of contact, this is essential, every notice of privacy practices must provide a point of contact to make that complaint within the organization. This is where I see a lot of organizations have outdated notice of privacy practices because they may specifically insert a person's name, their email address, and a telephone number.

Adam Bullian:

While there's nothing wrong with that what happens is that individual leaves the organization or changes jobs and now your notice of privacy practices doesn't have an appropriate point of contact in there. So what I recommend organizations doing is setting up a blanket email address, privacy at your organization, and including a general phone number, and then including somebody's title, the chief privacy officer, the CEO, the director of compliance. Something like that, that will be preserved as individuals come and go from the organization, and that email address and that other contact information will also be preserved so that you don't have to change your notice of privacy practices every time you have a staff change, and you don't have to then go notify everyone that has an outdated notice of privacy practices that this is their new point of contact.

Adam Bullian:

And the notice of privacy practices must be provided at times of service. This is certainly not true in emergency situations. If you're in an emergency situation you must provide a notice of privacy practices at the next appropriate time, so you don't have to obviously do it in the midst of an emergency. Providing that should be accompanied with an acknowledgement of a receipt. And so, in the resources that Andy sent out before the webinar yesterday it includes in there a model, a notice of privacy practices, that you can either use in your organization, or you can use as a check to make sure your notice of privacy practices includes many of the same elements.

Adam Bullian:

And also included in there is an acknowledgement of receipt, so you can begin to provide that to patients and that will come back to you so you now have a record not only that you provided the notice of privacy practices, and to whom, but that they read it and they agreed to it. The notice must also be posted in a prominent location. I see as I visit community health centers across the country, and I go to some of their non major locations, a lot of committee health centers as I know is probably true for many of the attendees today.

Adam Bullian:

You have locations throughout your community, some are larger than others. What I tend to see is that the smaller locations they don't have a notice of privacy practices posted. You need to have that posted in every location, in every site. If it's a mobile clinic it should be posted somewhere in there. Most often, it's posted in the waiting room. That's certainly most appropriate because that's where all if not the vast majority of your patients, and the folks that you serve, will enter and spend some time in that area.

Adam Bullian:

It should also be posted on your website assuming you have a website which most everyone I'm sure does at this point for your health center. It should also be posted there. So provided at the time of service in a prominent location most appropriately in every waiting room within your organization and on the website. And again, a notice has been provided to you to either use or to check what you have and make sure everything is there.

Adam Bullian:

So we'll switch gears now. I missed a question. So this is back from identifying what is PHI. The question is around whether the first name alone is considered PHI. The first name by itself is not PHI. If you just

say Adam, or Liz, or Andy, and assuming that there're no other identifying elements in there that would not be PHI.

Adam Bullian:

So now, we will switch to what are the three types of disclosures of PHI, and as I mentioned a few minutes ago this is something that I see a lot of organizations, not just health centers, they sort of constrict what they can do in order to protect themselves, and I certainly understand that, but I want to spend some time and identify the areas that are really required, permitted, and authorized, so that you know a little better of what you have access to do.

Adam Bullian:

Before we do that, one other question on the notice of privacy practices. In addition to having the point of contact you should also have a phone number and you don't have to say that is a way to make an anonymous report of a possible breach, or raise a complaint, but you should have a phone number as a way to contact in the event that anyone does want to make a complaint. So you would want to have all three of the primary ways of contacting your organization. That would be a phone number, a general phone number for the organization that would then connect them to the right individual, an email address, again, one that doesn't change when individuals leave the organization, as well as the physical and mailing address.

Adam Bullian:

So as we move through to the disclosures, so there're three types of disclosures. Required disclosures there are two types to the individual, and to the Department of Health and Human Services. There are permitted disclosures. These are things that are not necessarily that you have to disclose the information, but you may, and patient consent is not required, and we're going to dive deeply into each three of these. And then, there're authorized. Authorized is anything that does not fit in those first two, and anything that is authorized is essentially everything else, but it has to be accompanied by a specific patient authorization.

Adam Bullian:

So required disclosures of PHI as I mentioned, this is to the individual, you must provide the individual access to their PHI when it's requested, either if they want a copy of it, that must be done. If they just want to review it that must also be done. You also must provide access to the Department of Health and Human Services secretary when they are conducting a complaint, a review, or other type of enforcement action. Obviously, some of you may of been aware, but the end of last year, middle to end of last year HHS was conducting random audits. That would be a situation in which you could not bar or prevent the secretary or the department from having access to PHI. If they request it you must provide it.

Adam Bullian:

Also, I should note, because we have attendees from around the country, you may have specific state requirements that would require you to disclose PHI to certain state officials. Most notable this would likely be your attorney general. I would encourage you to spend some time and make sure. There are several resources out there to let you know what those are, but you may also have depending on your location required disclosures based on your state.

Adam Bullian:

So there are only two required disclosures. Most of everything else fits as permitted or authorized, and we'll spend some time talking about those at this point. And someone just raised a question about anyone else from HHS, like an OIG investigator, it's not only to the secretary. The rule says the secretary, I think, or designee. So essentially what happens is it's any of the offices within HHS that are operating under the authority of the secretary.

Adam Bullian:

For instance, the example that I gave on the random audits that were being conducted, those were done through the Office for Civil Rights. So it wasn't the secretary by name it was the Office for Civil Rights that was making those requests. But it's anyone really within HHS that would make a request of PHI. You would assume that they have the authority to do that. And you're free to dive deeper but most of the time if you get a request from HHS it's suffice to say that is a required disclosure.

Adam Bullian:

So now, we'll switch to permitted disclosures. These are things that you may do, you're not required to do, but if you choose to make this type of a disclosure you do not have to get the patient's consent or authorization to do it. I see a lot of organization that actually have the patient's consent to a long list of disclosures, most of which are the permitted disclosures. There's nothing wrong with that but it's not necessary. So most notably those are for treatment, payment, and operations.

Adam Bullian:

In my work with community health centers the bulk of their disclosures to individuals or most likely other organizations come in the form of treatment, payment, and operations. So it's most likely that they're not going to need any type of consent or authorization to do that. Anything when the patient has the opportunity to agree or object. What does that really mean? These are things like facility directories, if you maintain those. I also receive a lot of questions from people who ask what about a board in the waiting room that lists patient name. Something like that the assumption is that the patient could say they don't want that, and that is akin to a facility directory.

Adam Bullian:

So if you display the patient name, first name and last initial, or something like that, and then direct them to a specific window, or a specific door for check-in or for treatment that would be okay because presumably that is something that the patient has the opportunity to object to. If they did object you would then not put them in that system, and find a different way, a more anonymous way for calling them out.

Adam Bullian:

And also, commonly, we see when people dispense filled prescriptions to someone acting on the patient's behalf. That is a permitted disclosure. You don't have to get the patient to say I allow Adam to pick up my prescription. What you would have is it is generally permitted unless you have the patient say I don't want Adam to pick up my prescription.

Adam Bullian:

Things that are incidental to an otherwise permitted disclosure, so this is anything that might not be specifically permitted, but is incidental to that, to an otherwise permitted disclosure would be technically a permitted disclosure. Things that are in the public interest or public benefit activities when we talk about public health activities, reporting victims of abuse, which many of the clinicians have an obligation to do, health oversight activities, as well as law enforcement. So law enforcement investigations, or if you're disclosing information maybe for the treatment of somebody who is incarcerated, or otherwise transferred to law enforcement.

Adam Bullian:

Those are things that you may do without the patient's consent or a specific authorization. But again, you're not required to. And things that are in a limited data set. This is when all of the direct identifiers, all of those 18 elements, the identifiers have been removed. The thinking being it's no longer PHI. So those are the permitted disclosures. Again, things that you may do, you don't have to do, but if you do disclose this information for these purposes you don't need the patient to authorize that.

Adam Bullian:

So then, we get to the last one. So we've talked about required. We've talked about permitted. And now, we get to what is everything else. If it doesn't fit into those first two categories, if we haven't already discussed it, it has to be authorized specifically by the patient. It's any disclosure that's not required or permitted can only be made pursuant to a patient's authorization, and authorizations have to include specific things. They must be in plain language, so not legalese, it has to be something that patients can read and very easily understand regardless of their education level. If they have a hard time reading, or they may need it translated, that's something that should also be provided to them.

Adam Bullian:

It must be specific about the information to be used and disclosed, so not just saying that we're going to send everything regarding this patient to somebody, but we're going to send treatment notes with a start date and an end date, or only specific types of PHI. It must identify who is disclosing it and who is receiving it. It must state a time for the expiration. That time can be a specific date, it can be after a specific number of occurrences, or it can also be after a specific incident or event happens.

Adam Bullian:

What it cannot do is it can't be open ended. It can't say this is essentially in place until revoked. That's not permitted. But also, the authorization must permit the patient to revoke in writing at any time, so if the patient changes there mind then they have the opportunity to change their mind and for that to be carried out.

Adam Bullian:

I mean, it's hard to sort of describe all of the situations in which an authorization would be necessary. I put in too here a disclosure to an employer for preemployment physical. This wouldn't be a required disclosure. It's not to the individual, it's not to HHS, it wouldn't be one of the permitted disclosures. This would be something that would need to be authorized, and also potentially disclosing PHI to a pharmaceutical firm for manufacturing purposes.

Adam Bullian:

Another one that I have seen, and this sort of highlights the broad scope of what can be authorized. I had a community health center contact me and say they had a patient that sent them an authorization for their PHI to be sent to a journalist. Obviously, that's not something that's either required or otherwise permitted, and their question was "Can we do this?," and it can be done, and it really should be done, assuming there's no foreseeable harm that could be brought to the patient by that disclosure that you would know of, but otherwise if the patient authorizes it then you have to execute the patient's wishes.

Adam Bullian:

We have a couple questions on this topic so I'll pause here and address those. The first question is clarification on the need for the patient to sign a form as to which family members can be given information about them. So this is the second bullet here on this slide. This falls within the potential for the patient to agree or object notifying family on an individual's care. This is something that is permitted. You don't have to get the patient's authorization or consent to do that. If you are currently getting that consent that's fine, but if you have a feeling that it may be overburdensome then you're not required to obtain that consent.

Adam Bullian:

Some other things that you should keep in mind when it comes to family members is you always have to have in the back of your mind is are we potentially opening up the patient for any harm involved in making this disclosure. Obviously, when we talk about victims of abuse that may be something where you may choose not to permit that disclosure, and you even have the right, the authority I should say even if the patient authorizes those disclosures the community health center, the provider in any instance, really has the final say, and is this something in our best judgment is not appropriate for the patient.

Adam Bullian:

Now, that has to be backed up with real facts, but to directly answer the question you do not need the patient to consent assuming you have reason to believe that person is otherwise involved in the care or payment of the individual. So you can give them that information without signing a consent.

Adam Bullian:

Another question is, is it appropriate to disclose the address and current phone number of a patient that you learn is wanted by the police? I have to sort of put some rails around my response, and say I'm only going to answer this from a HIPAA perspective, and say that's something that would be a permitted disclosure. There may be some other instances in which that may not be appropriate but as far as HIPAA goes you don't have to get the patient's consent to send information, PHI specifically, to law enforcement about an individual.

Adam Bullian:

And if you think about sort of the policy behind that for a second that makes sense. If it's for national defense or otherwise public safety it's unlikely in most instances that the individual would consent to that type of disclosure, but there is a public need for that information to go into the hands of the authorities, so from a purely HIPAA perspective that would fall into being a permitted disclosure, and that would be appropriate.

Adam Bullian:

So I think I had another question on family members, and just to clarify you don't need to get the specific consent of the individual assuming you have reason to believe that those family members are involved, and you haven't heard specifically from the individual that they don't want that information to go to their family members, you could do that without the individual's specific consent. Now, if you have any question I would encourage you, and I've counseled several organizations on this in specific instances, have the clinician or somebody from your organization privately speak with that individual and say, even verbally, you can back it up with written consent that is it okay if we discuss this information in front of these individuals.

Adam Bullian:

There's nothing wrong with that assuming you have not question ... If you're discussing something with an individual, their family members are there, we're discussing PHI, then it is assumed that they had the opportunity to agree or object to that. If they don't object to that then you assume that they are agreeing unless there are other contributing factors.

Adam Bullian:

Another question. It seems that we have a lot of questions on disclosures, which is good. I may in a couple minutes if I can't get through them all I may continue on, and hopefully we'll be able to get to them at the end. I do want to make sure we at least get through the entire presentation. So another question is, if another provider's office request records from us is that a permitted disclosure without authorization even if it's not one of our referrals? That would fall into a permitted disclosure for treatment of an individual. You don't need to get the patient to authorize that.

Adam Bullian:

A question about PHI identifier, the date of service. Yes, if that's a specific date assuming it's a specific date of service, something more than just the year, that would be a PHI. That would be considered one of the identifiers. So I'm going to move on at this point and continue to keep those questions going. We'll leave some time at the end. I'll continue to address some questions on other topics as we move through. If we don't get through all of them at the end then we'll find a way to get those answers distributed after the webinar.

Adam Bullian:

So we're going to move to patient's right to access. The important thing to keep in mind here is that generally patients have an unfettered right to access to their own information. There's only two exceptions. That is psychotherapy notes. What is a psychotherapy note? Those are things that are not in the medical record, the electronic medical record, or really any medical record. Those are the personal notes made by a psychotherapist about an individual. Once that goes into the EHR, or any other record, about the individual that no longer qualifies as a psychotherapy note, and the patient does have access to that.

Adam Bullian:

So it's really the personal notes written by the therapist about the individual that don't actually make it to the EHR. So they don't have access to that, and they don't have access to anything that could present a danger to the patient. That's up to you, up to the clinicians, and your organizations, to decide what

that may be. And there's no real guidance in the rules, not much guidance, if any really, from the regulars about what would present a danger to the patient and thus limit the access that the patient has to that information.

Adam Bullian:

So if it doesn't fall within those two categories the patient has the right to access that, and they can access it in two most common ways. They can view it for free. You may not charge to view. If a patient requests just to view their information you may not charge them for that. That is strictly forbidden. If they need an interpreter you must provide them an interpreter to understand their PHI, the information that you have created about them. Most of the time, obviously, if you have a patient portal that is live this is something that can be done in the patient portal. It's done primarily seamlessly so it's not something that you really have to worry about.

Adam Bullian:

If you have a portal. Hopefully, gone are the days when a patient comes to the office, or comes to the organization, and asks to see their records. If individuals want a copy of their record you also must provide it to them in the form that they requested, so if they request it in paper you must print it and provide it to them in paper. If they request it to be emailed you should provide it to them in an email. The only thing that the rule says is that as long as it's not overly burdensome for you to provide.

Adam Bullian:

If it's overly burdensome ... And this is sort of a holdover before the vast majority of the industry was changed and had adopted electronic health records, but if you for whatever reason don't have an EHR, which I assume all if not most of you do, but if you didn't have an EHR, the patient requested it electronically that would be maybe the only exception of something that would be overly burdensome.

Adam Bullian:

So we have a question on fees, and I was just going to talk about fees. So you can only charge very limited fees on certain things. This is another thing that some states have specifically weighted in on, on exactly what kinds of fees you can provide, so I would encourage you to do some research in your own state about what those fees may be. And you can only charge a fee for a specific thing. Again, you can't charge a fee if the patient just wants to view it, you can charge a fee for a copy, but you can only charge a fee for the cost of actually making the copy. So if you're printing something in paper then you can charge for a per page cost, and for postage.

Adam Bullian:

If a patient wants it on a thumb drive then you can charge them the cost of the thumb drive. You cannot charge them for certain things like the time it takes you to collaborate it, or pull it all together, or the time it takes you to identify it, find it, and pull it all together. You can only charge them for actual things that are outlays, or costs to you, most notably copies and postage.

Adam Bullian:

We have some questions on right to access. One is they've had requests for records on CDs, but we use summaries without CDs, so would that be overly burdensome. I mean, if you don't have a way without going out and buying specific technology to make that CD for the individual presumably that would be

overly burdensome. If it's just a break from your normal operating procedure, but it's something that you do have the technological capabilities to do I would suggest that it's probably not overly burdensome. I would instead reach out to the individual, see if there's any way that they would be able to or willing to accept that in another form, maybe give them some other forms that you would like them to have, and then if they agree to that, great.

Adam Bullian:

If they stick by the fact that they want it in a CD, again, if you have the capability to do it you should provide it to them. What overly burdensome could also be considered is assuming you don't have to go out and buy new technology to do this but for a jump drive or the actual CD, something like that, then it probably isn't overly burdensome.

Adam Bullian:

Clarification is permitted to provide the patient with a copy of their lab records. During ambulatory care visit we don't charge them. Yeah. It's absolutely permitted. I mean, patents have access to the records assuming it's not a psychotherapy note and assuming it's not presenting any kind of danger to the patient, so if you're doing that, it looks like you're doing that for free, and then absolutely that is very much permitted and certainly would be encouraged by the regulators at the federal level.

Adam Bullian:

Interesting question. It's a little bit off topic because it's not specifically tied to patients rights but I think it's sort of tangentially related, it's about a third-party requesting information such as an attorney under a subpoena. Can you charge a fee for that? Again, this is something that can be dictated specifically by state, but generally, yeah, you can charge a reasonable fee. Again, it has to be tied to your actual costs to provide that, but yes, you can charge a fee to a third-party.

Adam Bullian:

When we're talking about the real restrictions on fees are around providing patients, and charging patients, or individuals access to their own information. Again, the policy behind that is one of the underpinnings of the privacy rule is patients should have access to their information.

Adam Bullian:

So I'm going to move on. I know there are a few more questions. I will try to get to those at the end as well. Again, I just want to try and make sure we get through everything. I do appreciate these questions so please keep them coming as we move to other topics as well. Another patient right in addition to the right to access is the right to amend. Patients have the right to make a request to make a change to their PHI. This can be something as benign as changing their address or other types of contact information, or we don't see this as frequently, but they can make a request that you change something like a diagnosis.

Adam Bullian:

And the important thing to keep in mind is you as the providers don't have to grant those changes. You as the providers, as the clinicians, your organizations are the experts here. The decision really comes to you, and the decision is yours. What the rule preserves is the right for the patient to make the request to make that change. What you also should keep in mind is that regardless of the outcome of the

amendment request you must document that. You must still take it under advisement. You must review it. And then, you must make a determination, yes, we will make this change, no, we will not.

Adam Bullian:

That means you should have a process in place to handle these as they come in. A lot of these, certainly the vast majority of them, would be things that you're going to do in the normal course such as changing names if somebody gets married, or divorced, or otherwise change your status, changing contact information, other such things you're going to change without any real consideration because that's the right thing to do. But if it's something that's a little bit more serious and actually goes to maybe a treatment or a diagnosis you certainly want to have a way to receive that request.

Adam Bullian:

You could have a form, a specific form, that they fill out so you can handle those in a very logical way, and a consistent way. That request for an amendment should be reviewed if that's necessary. Obviously, if it's something like contact information probably not necessary to really review it. You want to communicate what happened, the outcome of the review, to the patient. And again, this is another thing where states have weighted in, specifically California has sort of shrunk the time down to allow what time you have to notify the patient, and you have to notify them.

Adam Bullian:

So if you grant the amendment you must provide notice to anyone the patient asks you to provide that to, as well as anyone that you know needs it, so if you made referrals and you know that the patient hasn't also requested an amendment from those referral organizations, or those organizations that you referred and sent PHI to, then you should send an amendment to them if you know they would need it.

Adam Bullian:

The last of the three patients rights is patient's right to an accounting, and this is one that we don't see very often. This is one that if you pay attention to the happenings at the regulatory level you may have heard some talk about it in recent years about a potential change, but that change has not been made yet. So what is it? It's basically the patient can request an accounting of disclosures. That's essentially a list of all of the places that PHI has been sent to. This includes any transfers to business associates.

Adam Bullian:

And those transfers have to be documented, and you must keep a list of those for the last six years. So this often times brings about a good bit of panic because I know many organizations are not keeping this type of an accounting, and before you reach panic mode I just want to lay out the instances which the vast majority of instances you disclose PHI in which making an accounting is not necessary. If you transfer Phi for treatment, payment, or operations that does not need to be on the accounting of disclosures.

Adam Bullian:

If any disclosure is made to the individual, or their personal representative, that does not need to be included on an accounting. Anything that was disclosed to an individual who was involved in that person's healthcare or payment, so if you have other payment organizations that may be involved you

don't need to disclose that. Any disclosure that was made pursuant to an authorization you can assume that the patient knew about it or knows how to find out about it.

Adam Bullian:

Anything that's on a limited data set, again, those are things where the identifiers have been removed. Anything for national security or intelligence does not need to be on there. Anything to a correctional institution does not need to be included on an accounting of disclosures. And anything that has been incident to an otherwise permitted disclosure.

Adam Bullian:

So the vast majority of the ways, and the reasons, you disclose PHI don't need to be included on an accounting of disclosures. If you have disclosures, specifically ones that happen frequently, that would not be on this list of bullets then you should begin to put in place how you would make that accounting.

Adam Bullian:

So we're going to switch gears now again. I still know there're a lot of questions. I think we will definitely have some time at the end to get through a lot of those questions on disclosures as well as patients access, but we're going to switch gears again to get to the end.

Adam Bullian:

Who is a business associate? I've helped answer this question a lot for a lot of community health centers. So I've sort of taken the legal definition of what is a business associate, sort of made it into two questions that you could ask yourself as you're looking at an organization that is a potential business associate. You would ask yourself, does that organization in question perform some service or function on your behalf? And most of the time that's going to be a yes if they're one of your vendors. And do they need access to PHI to perform that service or function?

Adam Bullian:

If you answered yes to those, they're performing a service or a function for you, and they need access to PHI in order to perform that, then they are a business associate. So in now way can I put together an exhaustive list of potential business associates for community health centers, but I've tried to put together a list of the ones that I've encountered, the most common, and some of the ones that trip people up a lot as well. Certainly, your electronic health record vendor. They're a business associate of yours. A population health management tool which I know many community health centers are using, they're your business associate.

Adam Bullian:

Anyone who is your IT vendor. If you have somebody that does work on your EHR for you, any MSP. If they're outsourced, they're not a part of your staff, then they are your business associate. I also hear questions about payers a lot. So HIPAA's divided into essentially business associates, which is what we're talking about, and covered entities. Covered entities are healthcare clearing houses, providers, which is all of you, and health insurance plans.

Adam Bullian:

So I often get questions about payers, and most notably in the form of some type of nonprofit organization that is providing some funding to a community health center for the work that all of you do, and in exchange for providing that funding they ask the health center to send them some medical records or some type of information back to them to certainly audit and verify that good work is being done, which almost certainly it is. And that organization assuming that the information that is sent to this nonprofit if you will in this instance, if the information that is sent to them in exchange for the donation or the money that they sent to support you, if that has PHI then they're your business associate.

Adam Bullian:

Often people think that payers are the definition as a covered entity but it's not, it's health insurance plans. So if they are a payer essentially but they're not a health insurance plan, or they're not a go entity, then they would be a business associate. Also, consortiums that you share PHI with or PCAs, primary care associations. I see a lot of groups that contract with staffing agencies, and the individuals who you may hire, you may work with a staffing agency to provide nurses or physicians, or other types of staff to you, and certainly they are having access to PHI therefore the staffing agency itself would be a business associate.

Adam Bullian:

And this has recently been clarified by the federal regulators crowd storage vendors, so if your EHR's stored in the cloud that whoever is storing that is your business associate. The clarification that was primarily around if the cloud storage vendor does not have access to the information, for instance, if it's encrypted in the cloud and the vendor does not have access to the encryption key it's highly unlikely that they would have access to the actual PHI, but the clarification was that even in that instance, even if they don't have access to it, they still have a responsibility to secure it, and therefore they are your business associate.

Adam Bullian:

There could be many, many others. If you have specific questions feel free to include them in the chat box. Some common non-business associates are anyone with an incidental or a very limited access to PHI. Typically, we consider these to be any type of maintenance teams, or maintenance individuals, janitors, anyone that does not need the access to PHI to perform the function or provide the service to you. If they don't need the access, if they just see it in passing, or overhear it they're not a business associate.

Adam Bullian:

Also, conduits. This is what we think of with the phone company, postal service, FedEx, UPS, your ISP. It's in transit. It's not necessarily something they would have access to assuming they're doing their job in the normal course, not listening in on phone calls, or anything of that nature, so you wouldn't need a business associate agreement with those types of organizations, the postal service, your internet service provider, or your local phone company.

Adam Bullian:

So what is required from your business associate? First, there're a few things that are required mostly for. You must have a business associate agreement in place with those organizations before you provide them access to PHI. Now, if the water's already under the bridge, you're already doing work with them,

they already have PHI access and you don't have a business associate agreement with them that not a reason never to execute one, but going forward what you would want to do is to make sure you have those business associate agreements in place before you even send them information, or provide them any access.

Adam Bullian:

The business associate has an obligation to safeguard the PHI as it's outlined in the business associate agreement. We'll talk specifically about those agreements in a second. They must only access the minimum amount of PHI that is necessary for them to do the purpose that they've set out that has been stated in that business associate agreement, so they must limit their access, and you in sending them the information, or providing them access, should do everything within your power to limit their access to only the minimum amount that they need. They must notify you in the event that they have a breach.

Adam Bullian:

And number five here, this is not required, there's nothing in the rule that says you must do this. I see a lot of organizations, a lot of community health centers, and other organizations starting to be more proactive about their business associates. So it may be appropriate for you to conduct some type of a periodic review of those business associates to determine do they have the pieces in place to actually protect the information. You can do this in a number of ways. I know some organizations send out a generic security type questionnaire with a dozen, or two dozen, questions on it just to get some information on them before you ever execute that business associate agreement.

Adam Bullian:

You can also request copies of some specific types of records, any recent incident investigations that they conducted, their most recent security risk assessment, you could request that, and something like a training log. I'm a big proponent of training. I think training is one of the most important things that you can do, that any organization can do to really protect patient's information, and better implement your HIPAA compliance. So you can request their training log, make sure that they're training their staff regularly, they're training them at least once a year, they're training new hires as they come onboard. Something like that.

Adam Bullian:

What you're trying to do is number one prevent contracting and sending information to an organization that does not have the wherewithal or the capability to actually protect the information, and it's also to provide you with a little bit of insight into who are these organizations that I'm contracting with.

Adam Bullian:

Again, I should note that last piece is not required. You're not required to do any type of review or validation before sending organizations. We'll talk in just a second about what you are required to do. So these are the 10 things, this slide and the next, that must be included in all business associate agreements. We've provided, one of the slides in the deck, a link to a model business associate agreement that was put together by the Department of Health and Human Services. If you don't have one or you want to validate or verify that your business associate agreement is quote good enough, if you will, then check to make sure that it has these 10 things.

Adam Bullian:

You can also leverage that resource as a template that you can use, make some changes as necessary, and then you have a very good one. So what has to be included in business associate agreements, it must specifically establish what disclosures and uses are permitted by the business associate. It must specifically state that the business associate will not use or disclose PHI for reasons that are not permitted or required. It must require the business associate to implement the HIPAA safeguards necessary to prevent any of the unauthorized use of disclosure, require that they report to you any unauthorized use or disclosure.

Adam Bullian:

Some less common things that must still be in there require the business associate to disclose PHI to satisfy your obligations for an amendment or an accounting, which we just discussed a little bit earlier. So some covered entities use a business associate to provide the amendments or to provide any accounting. If you do that then they must do that for you if that's the reason that you've contracted with them. Otherwise, any of your requirements under the privacy rule, which we're talking about today, they must comply with that to satisfy your obligations. The business associate also has to make available to HHS any information to show your, the covered entity's, compliance with HIPAA.

Adam Bullian:

Number eight is an important one to consider. It must state what's going to happen at the termination of the contract, or the relationship, will the PHI be returned to you, or will it be destroyed by the covered entity. You must state that in your business associate agreement, what's actually going to happen at the end of this. The business associate agreement must require the business associate to also have business associate agreements with all of their subcontractors that they give access to PHI.

Adam Bullian:

They're no precluded from the business associate having a vendor but what they must do is they must also have a business associate agreement with that vendor. What we're doing is we're establishing a contractual chain of obligation and safeguard so that all along that chain as PHI is exchanged from organization to organization every organization is required to have the necessary safeguards in place.

Adam Bullian:

And number 10. It must state, and you're required, to terminate the contract, to stop providing access to PHI if you know that the business associate has violated a material term of this agreement, notably that they're not doing anything numbered one through nine. So if they're not disclosing, or they're pursuant to the business associate agreement, if they don't have the appropriate safeguards in place, and that's where that review of the business associate comes in then you have to stop that transfer of PHI, stop giving them access, and end the agreement.

Adam Bullian:

It's a very high bar I should note. It has to be actual knowledge. It has to be more than a suspicion. You actually have to know that they are not protecting the PHI. If you do get to that high bar though at that point you must stop that transfer.

Adam Bullian:

We have a question on business associates. The question says we have employees as patients in our organization. I think that's fairly typical. We use a third-party for HR management who have access to employee information unless we have a business associate agreement with them. Unfortunately, I need a little bit more information to answer this question and it depends on the type of employee information that this HR management company has access to.

Adam Bullian:

If they access to the protected health information, if they have access to anything that is created for the payment or provision of healthcare to the individual, and it contains one of those 18 identifiers, which assuming it does, then they would be your business associate. If it's other types of employee information then that crosses the line between PHI and goes to PII, personally identifiable information. This is what we talk about when we talk about credit card processing, education information, other types of financial services.

Adam Bullian:

There are duties and obligations that organizations have to protect that personally identifiable information, but if it's only personally identifiable, and it's not protected health information then HIPAA doesn't cover it. HIPAA only covers PHI, and for that reason if it's not PHI then a business associate agreement would not need to be executed. If it is PHI then you do need that business associate agreement. So again, unfortunately, it depends on the type of employee information. If it's PHI, yes, you should have a business associate agreement in place with that HR management company. If it's just personally identifiable information that this company has then a business associate agreement would not be necessary, but they still would be required to have some. Although not required by HIPAA there are some other requirements that they have to keep that information private and secure.

Adam Bullian:

So we're going to switch gears to our last topic now, and that is the discussion of policies and procedures. We're going to talk about a step-by-step way in which you can develop policies and procedures. First, let's talk about why they're important. I know in the work that I do with community health centers across the country that there are good practices in place on security, on privacy. You may have a good practice in place to provide patients access to their information, or provide amendments, or getting those notices of privacy practices signed and out to the individuals.

Adam Bullian:

What may not be happening is that you have the policies and procedures in place to specifically require that, and to explain to people, to staff I should note, to explain to staff why that's important and exactly how to do it. And that's important. It may seem trivial but it's actually important, specifically in times of staff turnover, or other crisis. So when we talk about natural disasters or other things, you may not have the full contingent of staffing available to you, they may actually need access at that very critical time to policies and procedures as they're filling in for maybe somebody else.

Adam Bullian:

It should also be available to stakeholders as a reference at all times. This is your opportunity to not just tell staff what's required of them but how they're supposed to do it. You're putting your staff on notice about what they need to do, what the organization stance is on certain things, but also how they need to go about doing it. So we can talk about the appropriate ways to store these things. In my experience

most organizations have a pretty good way of distributing all of their policies through an internal network, or some type of shared drive, or something like that.

Adam Bullian:

And while we're talking specifically about HIPAA required and necessary policies and procedures this can be handled in the same way as your HR policy and other policies, which may not be specifically HIPAA related. Policies certainly need to be periodically reviewed and updated. There's not a specific time. I think about every 12 months is good. If it's a new policy that's just been put into place something more frequent may be required, or may ne appropriate.

Adam Bullian:

And you should have one person in this personal role should be designated on the policy or on the document itself who is actually responsible for the care and maintenance of that document as well as the implementation. So it's that person who's responsible for updating. It's that person who's also responsible for designing it, and the initial implementation of that policy.

Adam Bullian:

So how do you go about putting these things together? If you know you need a specific policy, or you need a new procedure, how do you do it? So the first thing you should do is identify as we just talked about one person who's responsible. As the owner you should delegate that to them. If it's a privacy related policy consider somebody who's very much involved either if they're not the privacy officer as noted in your organization consider somebody who is very involved in medical record access, and providing patient's access to their information, somebody who has a strong understanding of what the policy nature is.

Adam Bullian:

It's also important from a regulatory compliance standpoint to know what the requirements are, and to know what's already in place. As we talk about HIPAA there are some things that are specifically outlined as you must do. When we talk about access, and amendments, and disclosure, accounting, certainly things that you must do or may not do, but a lot of times HIPAA's very broad because it applies to very large organizations, it also applies to very small organizations, everything across the board. HIPAA was intended to be flexible.

Adam Bullian:

So you need to know and be well aware of where do you have flexibility to determine what's right for us and for our organization, or where does the role specifically say I may do this, I must do that, or I may not do this. You also have to determine ... So you should also take an account, take inventory, or what's already in place, what's the organization doing. If it's something that you don't have a procedure in place for, but there is a process that goes on for that activity, for instance, you don't have a procedure on how to provide an individual's accounting, or an individual access to their PHI, but you are doing it, then you need to learn how is this done.

Adam Bullian:

What you want to do is not make a sharp turn in how the organization is doing things assuming they're doing things properly, and in compliance with the rules. What you want to do is big that procedure or

that policy around what's already in place as much as possible. And then, determine the organization's position. So the first three steps are really just getting everything organized, discussing here's what we need to do, here's where we have some flexibility, we can make the determination what's right for us, then that determination needs to be made.

Adam Bullian:

So now, in four and five the work really gets done. So this is where you actually draft the policy. Templates can be very helpful. Don't reinvent the wheel if you don't have to. There's an excellence resource. It's called HIPAA COW, it's a funny name, COW stands for the HIPAA Collaborative of Wisconsin, and I have a link in the resources slide at the end of this deck to their policy and procedure template library. It's all free for you to use. You can customize it. It's not customized by any state if you're not in Wisconsin. If you are in Wisconsin it is customized. But it is free for you to use, and it's for policies and procedures, and almost anything you would need is provided in that library. It's a fantastic resource.

Adam Bullian:

But you can leverage something like HIPAA COW's template library to give you a jump start on actually drafting the policy. Now, you have the framework. You have 80 or 90% of what you need, now you just need to make it customized for your organization. A significantly good headstart.

Adam Bullian:

So you'll draft the policy then next you would draft the procedure. Also, using a template is certainly helpful in that instance, but the procedure should be as specific as possible. What are the implementation steps necessary? There should also be an inclusion in the procedure about what types of logs or forms may go along with that. So if we're talking about the notice of privacy practices authorization policy include the acceptance. Include the acceptance form in that policy, so that not only does staff know our policy is to provide a notice of privacy practices to everyone to get that notice of privacy practices signed and get an authorization back from the individual, but here is the form that we are to provide.

Adam Bullian:

Once you have those drafts created you would want to distribute that to all of the stakeholders. You want to make sure to get feedback from anyone who's really going to be affected by this new policy or this new procedure, get their input, have a final approval. Often times I know that you must get final approval also from your board of directors. You may also have a compliance committee or some type of governance committee that it goes to before the full board. So get everything you need from the staff internally then provide that to a necessary committee, or the board of directors, get that approved, and then get it implemented.

Adam Bullian:

And also, the last thing to do as I mentioned policies and procedures need to be consistently reviewed and updated. So once that policy is approved by the board it's final, it's going to be effective in a certain time, set a time in the future. If it's a new policy as I said maybe three months or six months. If it's a minor update to an existing policy maybe look at it in another year. But put that on your calendar. Have an organizational calendar for policies and procedures so everyone knows when these things need to be

updated and reviewed, but do that when it's initially implemented. That's going to keep this process moving forward very smoothly.

Adam Bullian:

So here is a quick list of some of the policies and corresponding procedures that you should really have. You should have a password policy, and a password procedure, or standard operating procedure for passwords, saying things like it's our policy that we have passwords on anything that contains PHI. Our passwords have to be eight characters 10 characters, be specific. They have to be alpha numeric characters, upper and lower case, how frequently do the passwords need to be changed.

Adam Bullian:

I'm almost certain that your organization has a process in place and has outlined how frequently passwords need to be changed. The question is, is that backed up in a policy or in a procedure? Have a privacy policy. We've talked about access. We've talked about disclosures. We've talked about amendments. Those will often times be included in one sort of larger privacy policy.

Adam Bullian:

An acceptable use policy. This is acceptable use of the organization's technology, any desktops, or laptops, or mobile devices that are provided, what websites are they allowed to visit, are they allowed to check their personal email on work time, the things that outline in that acceptable use policy what is permitted, what is not permitted.

Adam Bullian:

You have a minimum necessary policy. This can be included in the password policy just saying that it is your policy that individuals that staff only access the minimum amount of PHI necessary to do their job. That's something that they have to do. You have to require that of them so it should be in a policy.

Adam Bullian:

A training policy. How do you train? Who do you train? When do you train? An incident response. It's not something we like to think about but you should be prepared in the event that you do have an incident or some type of a breach who's going to be investigating, how is this going to be handled.

Adam Bullian:

A mobile device policy, or a bring your own device policy, BYOD, if you permit that what's appropriate, do things have to be encrypted, so forth. All things that we'll talk in more detail about the webinar next week, as well as a sanctions policy. You should inform your staff if they violate a policy whether it's HIPAA or otherwise what are the potential ramifications for that.

Adam Bullian:

As I mentioned, here are the resources that we are providing. These are links, as you get the slide deck you can read up more on each of these. It's a general privacy summary by the Office for Civil Rights. There's the guidance on the notice of privacy practices, the sample business associate agreement that I mentioned.

Adam Bullian:

Number four is the HIPAA COW, the policy and procedure templates. A very valuable resource. Number five is a link to a blog that I write. I try to do something every week to give you some information that's actually practical that you can use, and that is hopefully appropriate and useful.

Adam Bullian:

So with that, I think we have about eight more minutes or so, so I'm going to try and go back and get to some of the questions that we have not addressed at this time. So if you still have some questions please get them in. If I don't have time to get to them all we'll work out a way that we can respond to those.

Adam Bullian:

So I have a question about resources for policies that are tailored to business associates. I would check the HIPAA COW, number four, on the resources. I believe that they also have information for business associates, but for the most part business associates really only have to worry about things on the security side, and most of those policies and procedures while they may be written from a covered entity standpoint could apply to something that is also business associate focused.

Adam Bullian:

I have a question about what would HIEs be considered, and so HIEs, they're not a covered entity, so they are a business associate. The disclosures for an HIE would fall into a permitted disclosure likely under the treatment, but potentially also under the payment, or operations categories. So they are a business associate but the disclosures to an HIE are permitted without need for patients consent.

Adam Bullian:

So another question that came in. If a patient is requesting all records for themselves we should not charge, would the patient need to sign an authorization or consent to release PHI? So you would only charge ... So a patient is, first of all, certainly permitted to request all information that you have about them, anything that's been created that you still have, so that's within the last seven years. You would want to provide them with that. What you would do is as the patient makes that request of access you would want them to fill something out, some kind of form, which would essentially be their authorization or consent.

Adam Bullian:

I would not get in the habit of just allowing the patient to verbally request access to their information, and you then provide it to them. I would want that documented on paper, so I would encourage you to do that. As far as the charge for requesting all records, again, if it's something that they just want to see, to view, that's something that you may not charge for. If they're asking for a copy that's something that you may charge for, but specifically only outlays of cost for copying, for postage, for purchasing a thumb drive if that's how they request it, for purchasing a CD if they want it on CD, something like that. So it has to be a specific cost.

Adam Bullian:

There are additional resources that are very specific at the federal level that go into exactly what the costs can be, and there are some limits as to how much you can charge for instance per page. But what's

also important to note is that you may not charge for say time to go find it, time to put it together, and things like that.

Adam Bullian:

So another question on payment for copies. It says you're having law firms request records electronically and they're saying that if they request them electronically we can only charge them the per page fee, is this true? So again, because it's a law firm and not the individual you have a little bit less constraints on what you can charge. In that specific instance I believe you can charge them a fee for pulling together that information, for finding it, but I also think because it's electronic, and assuming it might not be that hard to pull it all together, or to actually locate it, I think the best case would just be to charge that per page fee.

Adam Bullian:

So a good question on sending information a patient requests by email. Are there security measures that need to be in place? First of all, I would say if you have a specific question about this that's a good one I would encourage you to attend next week where we're going to get more into the security rule, and specifically exchanging PHI by email whether that be with the patient or with somebody else.

Adam Bullian:

So high level, it's permitted to exchange information via email specifically with the patient and even more specifically it should be done if they request it that way. What you should do before you exchange PHI through email is have the patient sign an authorization, or a consent really, that says this is how they want their PHI shared with them, and that they understand that there are risks that they may have an unsecure email inbox, but they understand those risks, they accept them, and they still want the exchange to go forward.

Adam Bullian:

Assuming you get the patient to sign that you're in very good shape. You would not be on the hook for any inappropriate access once it reaches the patient. So if they're using Gmail, or Yahoo, or some other otherwise unsecure email, and that's hacked it would not be your responsibility. Once it's transferred to the patient the responsibility transfers also to the patient to protect that information. Obviously, you still have to protect the information that you hold, but now the patient essentially has a copy, and that copy is their responsibility to protect.

Adam Bullian:

So I think we're just about out of time. I'll turn it back over to Liz and Andy. I think we still have some questions outstanding, and I will defer to the two of you on how you want to handle that.

Elizabeth Zepko:

Thanks so much, Adam. So for those questions that we did not get to respond to what I'll do is save this Q&A and we will get back to you in writing once we get these questions off to Adam. We actually want to thank him for joining us and we look forward to next Friday's webinar. Folks, registration is still open for the webinar on the third. If you'd like more information please visit our website, or you can send us an email personally to Andy, and receive some more information with that.

Elizabeth Zepko:

Once you close out of Webex today you'll receive a brief survey. Please let us know what you thought about today's webinar. We're going to use some of that information to tailor next week's webinar based off of your feedback. Thank you so much. We hope that you all have a fabulous day at your health centers and we'll speak to you next week. Thank you so much. Bye everyone.