Transcription

Media File Name: Data Security.mp3
Media File ID: 2678872
Media Duration: 53:50
Order Number: 1936200
Date Ordered: 2018-09-27

Transcription by Speechpad
www.speechpad.com
Support questions: support@speechpad.com
Sales questions: sales@speechpad.com

Megan: Hello, everyone, and welcome to this, "Ask the Expert" webinar on health information privacy. I'm Megan Hiltner with the Healthy Start EPIC Center. We have approximately 60 minutes set aside for this, "Ask the Expert" webinar. It's being recorded, and the recording, along with the transcript and slides, will be posted to the EPIC Center's website following the webinar. That website is healthystartepic.org. We really want your participation, and we've included some polls in this webinar. But at any point, if you have questions or comments, please chat them into the chatbox at the lower left corner of your screen. We also want your feedback following the event, so please take a moment right after the webinar, and complete the survey that will pop up on your screen.

This webinar evolves from questions and comments that we received from TA requests or technical assistants' request, and through discussions at regional meetings. And during the webinar, you're gonna hear more about HIPAA provisions and data security requirements as they relate to Healthy Start programs. We'll also get into data sharing and really look at, for example, how you manage client referrals with regard to HIPAA, and dig deep into privacy notice. This webinar is specifically for grantees that aren't located at an FQHC or a Health Department. If you are located in FQHC or Health Department, you can consult your office for HIPAA training.

So let me introduce your speaker for today. The presenter is Ms. Patty Depidova [SP]. She's a senior consultant at JSI and has been providing HIPAA training across the country through JSI's work with community health centers and other healthcare providers. I wanna let you know, Patty definitely knows her stuff. She is not a lawyer, though. She will not be answering any legal questions, but I guarantee you, again, she does know this content area.

So before we get started, we wanna do a really quick knowledge check. So, if you'll take a moment and respond to this knowledge check question to the best of your ability. So I'm gonna read the question, and the poll is showing up on your screen there. "HIPAA only applies to covered entities, which include, A, health plans, B, healthcare providers, C, healthcare clearinghouses, or, D, all of the above." So what do you think is the correct answer there? I'll give you a moment to respond, and by doing that, you just click on the radio button next to the responses. I see about eight of you have responded. I'll give it one more minute here.

Okay. All right. Looks like everybody thought the answer was D. So we're gonna do one more knowledge check question, and then we're gonna go through the presentation, and at the end of the presentation, we're gonna ask you these questions again, and see if any of your responses have changed.

So then the next question we have here is, and there's a few abbreviations here, but I'm going to read the question out loud. "Which of the following is required to be included in a privacy notice by a covered entity? Is it, A, a list of providers that the protected health information or PHI could be shared with? Is it, B, a copy of the entire HIPAA legal document? Or is it, C, how the covered entity may use and disclose protected health information?" What do you think? I see people are chiming in. And give it one more second here.

Okay. And it looks like everybody thinks it's C, how the covered entity may use and disclose protected health information. I'm not gonna give away the answer just yet, but we will be getting more into the...Patty will be covering this content in our presentation. So listen close, and see if your answers change by the end of this. So I'm turning it over now to Patty to begin our presentation. Patty?

Patty: Hi, everybody. Thanks for joining us. I just wanted to give you an idea of what the objectives are, and just to state, first of all, this is just a broad overview of HIPAA. It's kind of just a taste. You may be aware of a lot of the things we're gonna talk about, and some of them might be new. But to really delve in to the requirements of HIPAA, it would take probably a day-long session as a minimum, plus the time you would need to develop policies, procedures, and other documents. So this is really a high level overview, and the objectives are really to build an awareness of not just HIPAA, but also privacy and civil rights law, of which HIPAA is one of those, and to explain patient privacy requirements and guiding principles, and to be able to describe the responsibility of a covered entity.

Next slide. So the main takeaways, and I can't really emphasize this enough, is the very first one is use your common sense. Treat people's information the way you would want other people to handle your health information. And I just wanna go a little deeper into that. There are some issues where people use HIPAA, or not a firm understanding of HIPAA, to actually keep information from being shared that would benefit someone's healthcare or someone's services. So it's really, really important not to overdo it with HIPAA or any other privacy requirements, but just to meet the standards that are set up. And then the other takeaways are so, you know, we're gonna talk about some policies and procedures, not all of them, and some of the documentation that's required to comply.

Next slide. So as I said, HIPAA is a subset of privacy and civil rights laws, and it's really important to be aware of all of the ones that could impact the work that you do and the state that you're in. The federal laws include HIPAA, and

that's what we're gonna talk about most in this webinar, so I'm not gonna define it here, but we'll spend the rest of the webinar talking about HIPAA. But you also need to be aware of the confidentiality of alcohol and drug abuse patient records. It's often referred to as Part 2 because it comes from 42 CFR Part 2. It's similar to HIPAA, but it's slightly different. There's some overlap. Also, other federal laws that can apply are the Title II of the Americans with Disabilities Act, or ADA. And in terms of educational records, the Family Educational Rights and Privacy Act, or FERPA. This is not a conclusive list. It's, again, just touching on some of the bigger laws that are out there, and there may be others that may impact the works that you do as well.

Some of the state laws that can be in place, and again, it's different from state to state. So it's important to know where you're operating, what those requirements are. Very common ones are doctor-patients and therapist-patient privileges, communicable disease reporting to public health entities, and there could be specific laws relating to minors, in terms of some of the work that you may do. So it's important to be aware of those. And we are not gonna go in-depth with any of those laws. So, but I just want you to be aware that they're out there, and they can impact the work that you do. And in some states, the state law may supersede HIPAA even. And HIPAA may supersede the state law. Usually it depends on which law protects the individual's privacy the most, and that would be the law that would be in effect for the particular issue.

Next slide. So we have another poll, "How comfortable do you feel about HIPAA as it relates to your work?" The first choice is, extremely comfortable, somewhat comfortable, or I don't know anything about it. [crosstalk 00:08:58].

Megan: So, folks, if you'll take a moment and chime in. Yeah. It will really give Patty some understanding of how in-depth to go on some of this stuff, and I see folks have chimed in. Looks like a mix here.

Patty: I would say great.

Megan: Yeah.

Patty: Great. Okay. Next slide. So the HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. There are five main rules that comprise HIPAA. The first one, and the one that people think of the most when they're talking about HIPAA, is the privacy rule. The privacy rule established national standards to protect individual's medical records and other personal health information, which we just call PHI. This is the rule that most people refer to when they're talking about HIPAA, and it's the one we're gonna be concentrating on throughout this training.

The second rule, the one that took place, was the HIPAA security rule. And that's the one that's really talking about those safeguards, like administrative, physical, and technical safeguards to ensure confidentiality, and also the integrity and security of electronic protected health information. The third rule that went in place was the one that established national identification numbers or identifiers, and they're called NPIs, and you've probably heard of those providers. Each have a unique NPI number that they carry with them throughout their career, which is different than the way it used to be where they would have a number for each health insurance that they would take, different numbers for their life insurer. And those can all change over time or from state to state, whereas the NPIs follows them throughout their career and from one state to another so that their work can be tracked.

The fourth rule is that for the transaction and code sets, and that established standard transactions for electronic data interchange of healthcare data, and adopted standardized codes for diagnoses and procedures. The fifth rule, and we'll touch on a little as well, is enforcement. These are the civil and criminal penalties that may be assessed to ensure that HIPAA rules are followed and that organizations are in compliance. There's the source at the bottom, which gives you a lot more information about each of these specific rules. Again, we're gonna really concentrate on the first one, privacy.

Next slide. And next slide. So the HIPAA privacy rule sets standards for when personal health information can be shared by establishing permitted uses and disclosures. The most important terms to understand are covered entities, the covered entities' business associates, and protected health information or PHI. That's because the HIPAA privacy rule only pertains to covered entities and business associates, and then the way they use or disclose protected health information in their care.

Next slide. So covered entities are in three categories. This was some question at the beginning of the poll. They're either health plans, healthcare providers, or healthcare clearinghouses.

Next slide. The health plan that is a covered entity is pretty basic. It's commercial health insurers or managed care organizations, or government insurers, like Medicaid, Medicare, and the VA administration or Veteran's Health.

Next slide. Providers are a little bit of a different definition than we might normally think of them. This is the legal definition. A provider is either a person or an organization. So really a hospital would also be a provider, or a

health clinic that a provider works in. And some of your agencies may also fall under this category. They may or may not. But a healthcare provider is a person or an organization that furnishes bills or is paid for healthcare in a normal course of business. And the important thing, the and, is they also transmit health information in electronic form. I think it's important to note that if you're a covered entity that is the healthcare provider and you fall under this definition, that even though the definition says transmits health information in electronic form, it will then pertain to all health information, including the written word, verbal information. But this definition is just to qualify who is a healthcare provider and who is not.

It's possible that there could be a healthcare provider, a physician, a physician's assistant, nurse practitioner, who might be working in some kind of a category in the United States where they're not doing this. They're not furnishing billing or paying for healthcare in the normal course of business and not transmitting electronic health information. In that case, then they wouldn't be considered covered by HIPAA. Even though they are a healthcare provider, they would not meet this definition. An example might be someone who is a parish, a nurse practitioner working in a church parish and not billing for anything, providing free care, and not transmitting information electronically, having a paper chart. So that would be someone who's not a covered entity because they don't meet this very prescribed definition of a healthcare provider.

Next slide. So healthcare clearinghouses are, basically, big data organizations. So the best example is a billing service that processes data in a standardized billing format.

Next slide. So if you're curious about whether or not you're a covered entity… And the Healthy Start grantees, in many cases, may be very directly a covered entity, and in some cases it might be clear that you're not. But there might be a lot of gray areas. If that's the case, it's really worthwhile to get on...so the tool here that this is...I'm sorry. There's a link here, so a tool through CMS that walks you through all the questions to ask to decide whether or not you're a covered entity. Again, you know, I would go back to one of the first slides to use common sense. Even if you're not a covered entity, you're gonna wanna treat people's protected health information the way you'd want your health information treated. The difference is, and we'll get into that a little further is covered entities are required to jump through a lot of hoops. So if you're not a covered entity, you really should know that because you wouldn't have those requirements. But if you are a covered entity, you wanna be in compliance. So it's a good idea to get on this site. And if this isn't clearly defined for you, the next step might be to consult an attorney who might help you figure out whether you need to comply.

Next slide. So we have another poll, "Have you ever used the covered entity guidance tool?" The one we just discussed.

Megan: So if you've seen it before folks or looked into something like this before, let us know. We were curious. It looks like, Patty, most folks have not seen it yet, so it might be worth you all taking a look at.

Patty: Definitely. It's definitely worth checking out. Even if you don't actually use the tool, it might be worth taking a look at the questions and start thinking about that within your organization.

So the next definition that's really important to understand in terms of HIPAA is the business associates. So business associate is not a covered entity, but it's an organization or a person that might support the covered entity by performing functions or activity that involve the use or disclosure of protected health information. So they're working for the covered entity or is contracted with the covered entity, and may either come in contact with protected health information, or actually be responsible for doing something with protected health information.

So the examples that we're given here are someone doing data entry on behalf of a Healthy Start worker, assuming again that that Healthy Start program has determined that it's a covered entity. If they're not a covered entity, then that person would not be a business associate. Or an enrollment specialist that's enrolling participant in the health insurance plan. Again, only if that they're providing those enrollment services for a covered entity. So it's kind of a branch of a covered entity. There has to be a covered entity in order for the business associate to exist.

Next slide. So covered entities need to...it needs to be really clear...I'm sorry. It's not the covered entity. The business associate has to satisfy a number of things in order for the covered entity to make sure they're compliant with HIPAA. So the covered entity has to get assurances from the business associate, or BA, that they will use the information only for the purposes for which it was engaged by the covered entity, that they'll safeguard the information from misuse, and that they'll help the covered entity comply with their part of the HIPAA privacy rule.

Next slide. So the best way to do that is through a business associate agreement because the covered entity has to get the satisfactory assurances in writing, and that's best done through a contract. The business associate agreement can be an attendance with existing contract. So if you're working with a transcription

service, for example, they already have a contract, the business associate agreement could be a few pages that are just added on to the end of the contract. It doesn't need to be a separate document.

But the business associate agreement, or BAA, describes the permitted and required uses of protected health information by the business associate. Sorry, there's some duplicate words in here, but...and also requires the business associate to use appropriate safeguards to prevent a user disclosure of protected health information other than the way it's supposed to be used according to the business associate agreement.

So, basically, the covered entity is saying, "I'm contracting with you. You're going to either handle or have access to protected health information, and I need you to assure me that you are going to comply with all HIPAA compliance regulations, just like I would have to as a covered entity." There's a sample business associate agreement. There's a link to it at the bottom of this slide. I would advise you to look at it. It's very well-written, and it has some places where it suggests where you might want to modify it to customize it to your organization. They're pretty simple to put together.

Next slide. So what's protected health information, or PHI? So it's information that's either created or it's received by a covered entity. It relates to the past, present, or future physical or mental health or a condition, or it relates to the provision or payment of healthcare of an individual. And it's identifiable. It identifies the individual, or there's a reasonable basis to believe that the information can be used to identify an individual.

Next slide. So this slide, you don't really need to know everything on here. Again, once you're a covered entity or a business associate, but these 18 different factors have to be considered in terms of de-identifying protected health information. So just because you leave someone's name off something doesn't mean that it's not still protected health information. In fact, for the second one, the geographic subdivisions smaller than a state, you can only use the first three digits of a ZIP code. You can't use the whole ZIP code. And if you have those 3 digits and all the people that live there are less than 20,000 people, in a 3 digit, the first 3 digits of the ZIP code, you can't even use that. So you have to be really careful that you're complying with these specific factors.

For the third one, there's an asterisk there about all elements of dates. Dates can be used. And those are things like birth dates, admission dates, discharge dates, and dates of death. However, if the person is aged 89 or over, you can only use a year. You can't use a month and a day. So it's to make sure we're not putting things in such small population categories that someone could be identified. So

I won't go into each of these. You'll have the slides if you need to take a look at them. But it's really important to be aware of the types of things that can identify someone and not just be thinking of their name and address, those kinds of things.

Next slide. So how do we...what are the permitted uses and disclosures for a covered entity or for a business associate? The first one's pretty obvious. You can give the information to the individual that it's about. It's their information. If they want their information, then they are certainly able to receive it. The other big one is for treatment, payment, or operations. If you are functioning as a healthcare provider, a clearinghouse, or a health plan, then anything that has to do with taking care of a person's health, mental health, or physical health, that involves treatment payment or operations, operations of a clinic or a facility, organization, if those things are necessary for that, then that is a permitted use.

This is frequently an area that people misinterpret. They think HIPAA means they can't ever give out information. But it can really impact someone's health if these uses and disclosures are not considered. So, for example, if someone sees…and I'm not gonna be able to get a great Healthy Start example here because I'm not sure which of you may be covered entities. If a primary care provider referred someone to a cardiologist, they don't need to get an authorization to send out the referral and any health information, including a complete medical record, to the cardiologist. Because that's part of treatment, and they can also give that information to health plans. They wouldn't give any more information than is needed, but if the referral requires an approval, a prior approval from the health fund, then they need all of that. Or if they're doing some quality improvement initiative in their organization and they need to be able to see that data, that's okay as well. So these are the things that do not require an authorization specifically from the individual for whom the PHI is for.

The third thing is, clearly, if there is a valid authorization that's a permitted use and disclosure. The fourth one is when...I do some work with emergency preparedness, and this comes up frequently [inaudible 00:27:30] and would also come up with hospitals. It is okay to have a facility directory available that can be shared with a relative or close friend or other person identified by the individual. So, for example, a hospital can have a directory of who is an in-patient. A shelter, that is a healthcare shelter or a healthcare proxy, something that was set up in an emergency situation, can also have a facility directory. The important thing to note is that if someone does not wanna be on that directory, they have the right to withhold that information. But the onus is on them to make sure that they've told the organization they don't want their name on the directory, and that may come up in cases of abuse or, you know, where people

do not want their location identified. But without them making that discrimination and notifying the organization, it is a permitted use and disclosure without an authorization.

And then the last one is kind of a catch-all, where uses and disclosures don't require consent. Excuse me. And that may be some local laws or there may be some very specific things, and some of those will come up on the next slide.

Next slide. So when consent is not required, the first one is to avert a serious threat to health or safety. This is something that came up in Katrina, where sometimes data was needed. You know, pharmacies needed to be able to get prescriptions to people, and there was...you know, it was not possible to make sure they could get consent. Information was needed to be shared amongst organizations to avert a serious threat in an extreme situation. So, you know, there are times when it's just not gonna happen, where people's health is much more important, and their safety is more important, and you have to deal with those situations first.

Second, as required by law, again, there may be some specific laws where consent would not be required. For public health activities, so validations of infections, coming in and doing, you know, some TB work where there may be situations where there's tuberculosis going through the community. So those of types of public health activities. Coroners, medical examiners, and funeral directors, organ donation, and then some specialized government functions, such as military and veterans' activities. And then the last one is for worker's compensation.

Next slide. Okay. Now we're gonna talk about the requirements if you are a covered entity, and I can't stress that enough, if you're not a HIPAA covered entity, these are not requirements that you have to comply with, but you should try to figure out if you are. So this is, again, a long laundry list. This will be part of a much deeper, longer training. We're not gonna go into all of it, but if you're a covered entity, this is kind of a laundry list of what you need to do. We've talked about the business associate agreement, which is the third one down to amend the contracts that you have with your business associates to make sure you've included those provisions.

And we're gonna talk about the last one, develop and disseminate a privacy notice. But you'll notice there are a lot of things here that require policies and procedures to be put in place regarding medical records, and being able to track medical records to see who's gotten into a medical record at any point of the day, and stamp that by time and date and who it was. And giving individuals the right to inspect and amend their records. There are a lot of procedures and

policies that would be required. But again, if you're not a covered entity, they're not required, and we are gonna really be talking out just about the privacy notice. That's the big time-consuming requirement.

So, next slide. And so the privacy notice. What needs to be in a privacy notice? You've all signed this, I can tell you now. You signed them not only with your healthcare providers, but thanks, they gave you a privacy notice, usually annually. And your healthcare providers give you one when you...usually your first visit, and then often, every visit, just to make sure you've gotten it, or at least, annually. So what needs to be in it? Basically, how that covered entity may use and disclosure protected health information. So, there are ways that the covered entity may use and disclose protective health information if they inform you in advance. Marketing is one of the major things that can be in that, but usually it's not. But it's a good idea, if you are covered entity, to look at all the ways you might, in the future, even if it's not now, but in the future, you think you may need to use or disclose protected health information.

The privacy notice would also include individual rights with respect to the protected health information, how they should make complaints, and what the covered entity's legal duties are with respect to protected health information and contact information. So let's say, if they have other questions, or to get further information about the covered entity's privacy policies, and also the effective date. If the covered entity decides to make any revisions to the privacy notice, they will need to redistribute that privacy notice to everyone involved and make sure that it's posted appropriately. The law regarding the content is listed here if you wanted to take a look at it for more detail.

Next slide. There's a great website, hss.gov, it's listed here with kind of the picture of it, that has model privacy notices. They're in different types of format, so they can meet whatever needs an organization may have. There's a booklet. There's a layered notice. There's a full page notice, and then there's one that's text only. There's instructions for covered entities. In terms of crafting the privacy notice and making sure it's customized to their organization, and the model notice you have available in both English and Spanish. So this link would give you access to all of those model notices.

Next slide. So here we have another poll question. "Do you have a sample privacy notice that you'd be willing to share with other grantee? Yes or no?" If you could all answer that, we can take a look.

Megan: Looking like the majority of the group does not have one that they have. So that website might be an important resource if you're looking for a template.

Patty: Might even be just work with…you know, even if you're not a covered entity to kind of...it doesn't hurt sometimes to look at the specifics [inaudible 00:35:46] make sure that you kind of have this thought process with your organization to make sure you're protecting things the way you think it should be protected.

So how does a privacy notice get distributed? For covered entities with a direct treatment relationship, it should be distributed with the first encounter. This is from the laws of [inaudible 00:36:13] patient, and I know that you have clients or participants, so you can substitute that word in, but this is coming directly from the law. So the first encounter would be the first point of distribution. It should also be made available electronically through either a patient portal or another electronic service, through prompt mail, a telephone service. It should be posted at all service delivery sites, posted on the website. It should be available to anyone who asks for it, whether or not they are a participant in your program. So somebody walks in off the street, you need to have it available.

And I'm sorry, I think my computer is rebooting. So I'm gonna ask you to keep going ahead, and I'm gonna go from my notes.

Megan: Sounds good. That's what we're here for, Patty.

Patty: Yeah. All the patches just uploaded to my computer. So, and you need to make a good case effort to have acknowledgement that the person who got the privacy notice actually received it. A lot of organizations will have a spot where people have to sign that they received the privacy notice, whether or not they wanna take it with them. I know I rarely take it with me.

So the next thing we're gonna talk about is the business associate agreement. We talked about it a little bit. Again, I think some of these is duplicative. So I think we're gonna move ahead. Looks like two slides were in there twice. We're gonna move ahead to slide 34, enforcements. And this is the part I said I was just gonna touch on a little bit. There's a lot more information, and you can see it on this, on the sources that are listed for HIPAA compliance, but there are non-compliance penalties. HIPAA is very serious business. Again, no one wants their private information to be available to people that they don't want to see it, so there are financial and criminal penalties for noncompliance. The penalties can be applied even if there is not a breach of protected health information but there's noncompliance.

So the most common one for that is having no business associate agreement in place, which is one of the reasons we're really talking a lot about privacy notice

and business associate agreements. So if you don't have a business associate agreement in place, but you didn't even have a breach of protected health information, you're still not in compliance. An ignorance of HIPAA rules is not an excuse for rule violation.

Okay, next slide. It should say breach responsibilities at the top. If there is a breach, it's really important to conduct a breach risk assessment. And then once the risk assessment is conducted, it's important to notify the impacted individual. So, breach risk assessment involves examining the nature and extent of the protected health information that was involved in the breach, including the types of identifiers and the likelihood that someone would be re-identified. And also checking to see who the unauthorized person or persons were, who used or could see the protected health information, whether the protected health information was actually acquired or viewed, or there was just a risk that it might happen. And the extent to which the protected health information risk has been mitigated. So all those things added together would be the breach risk assessment.

So then it's up to the covered entity to notify without any reasonable delay the affected individuals, or they need to show that they do not need to notify the affected individual because the risk assessment shows that they really...they may comply with some exceptions to the rules. So one exception would be if two people in an organization who both were HIPAA trained worked on potentially different projects and mistakenly someone saw something on someone's desk that they shouldn't have seen. They told him they shouldn't have seen that, but they both, you know, were HIPAA compliant in every other category. That would be an exception. That wouldn't be a breach that would need to be reported.

It's interesting that when I look on my...I live in New Hampshire, and I looked on my state records for breaches, because they have to be reported publicly, and some of the breaches in my small state involved 50,000 people or more at a time. So breaches can be significant because of the nature of electronic data. So those are really...I mean, any breach needs to have a risk assessment and followed up, and individual patient needs to be contacted. But you do really do need to do that risk assessment to get an idea of really how big the damages are.

And we're now in slide 37. It starts with "remember." So remember, protected health information can be disclosed for treatment, payment, and operations, to prevent an imminent threat to health or safety, and for identification, location, and notification. Really important not to forget that because there have been a number of cases. There was a breach in issue of the Journal of the American Medical Association I believe it was in June or July, that had three articles

discussing this topic, and about how some people are not getting the appropriate healthcare because people are too worried about HIPAA, and they're not following HIPAA standards. They're going even further, and it's not what the law was meant to do. It wasn't meant to deprive people of healthcare. It was meant to keep their information safe.

So it's really important not to overstep the law. I had a good example where I was trying to make an appointment for one of my adult children with their doctor, and they wouldn't let me make the appointment, and I had to remind them I was providing them with information. They weren't providing me with any information. So it can really kind of go too far sometimes, so it's really important to just follow the law and not try to go way beyond it. But in all circumstances where you're unsure, try to get consent when you can. Then it's the protected health information provided to the minimum necessary to get the job done, and make sure you have the policies and procedures in place that are required by law, particularly if you're a covered entity or a business associate.

That's the end of kind of my formal slides. I'd like to open it up for questions now.

Megan: So, Patty, there were a couple of questions that were submitted, and the first one, it goes into the slide where you were defining covered entities, and you were defining healthcare providers. So the question is, do Healthy Start case management services count as being paid for healthcare in the normal course of business?

Patty: Again, I think you need to get on...I'm not a lawyer, and I don't work with Healthy Start grantees exclusively, I've done a little work with Healthy Start grantees. So I think you really have to look at what types of services you're providing, whether you meet the definition of being a provider, a healthcare provider. And the best way to do that is to get on and use that tool. If you use the tool and you still can't decide, it really is worth having an expert, a lawyer, give you some advice.

Megan: And that tool, folks, we put it into the chatbox, but it's the CMS tool, and we can rechat it. If you want it, let us know. Oh, there it is. Okay. So then the second question, Patty, and we, I remember in our planning for this call, kind of discussed this. So you may not have the answer, but I'm gonna put it out there in case other folks have the same question.

Patty: Sure.

Megan: It's about the slide where you were going into the de-identifiers, where you had the list, and I can pull that slide up while we're talking about it. Where is that over back? Here it is. So the person said, this list reaffirms concerns about submitting our client level data to the Healthy Start monitoring and evaluation database, that it's been said that the information is, "De-identified," but it contains a lot of these identifiers you list here. And so this group, this is Valerie, I hope you're okay with me putting your name out there. This is Valerie Gearson Rocherster said that they've developed a revised consent form that really explicitly notes that they'll be able to...they will be submitting client level data. So it's more of a comment, but anything else you wanna share on that?

Patty: You know, I think that's always a safe thing to do. Clearly, when you have a consent form, it's fine. You can provide the information. I still think you need to also look and realize that you need to look at what that relationship is, and if it is being provided for public health information, to a governmental body, it may also be an exception. And also you need to look at just because it has these characteristics, if you're not a covered entity it's not protected health information. So it really goes back to figuring out whether you're covered entity or not.

So, for example, if I went to Weight Watchers, they'd have a lot of information about me. They'd have my weight. They might have asked me if I'm on any medications. They have my name. They have my address. They'd have all kinds of things that I might consider protected health information. But they're not a covered entity. So it's not covered under HIPAA. So you really have to go back to that first question of whether or not you're a covered entity. Hope that helps.

Megan: All right, thank you. That's great. That's great. Any more questions, folks? There's no more questions or comments in the chatbox right now, Patty, so I'll just...we'll kind of give it a moment.

Patty: Sure.

Megan: Maybe while we're giving it a moment, let's go back to our knowledge check and see if anybody's questions or responses have changed. So the question, again, folks is, "HIPAA only applies to covered entities which include, A, health plans, B, healthcare providers, C, healthcare clearinghouses, or, D, all of the above?" What do you think? I'll just click in on the radio button. Looks like folks are figuring that out quick. Okay. And people's answers didn't change. And that is the correct answer. It is all of the above.

All right. So then the second question here is…let me find the full notes so I can read it to you. Okay. "Which one of the following is required to be included in that privacy notice by a covered entity? Is it, A, a list of providers their protected health information or PHI could be shared with, a copy of the entire HIPAA legal document, or how the covered entity may use and disclose the protected health information?" We'll see how you'll respond to this one. It looks like one person thought that it was a provider list that the protected information could be shared with. The answer is actually C, or the last one, how the covered entity may use and disclose the protected health information, so.

Patty: So just...

Megan: Go ahead, Patty.

Patty: Just to go back to the last question, where they talked about how getting consent upfront to release the data to HRSA, the other thing that might be considered is to include that in your privacy notice. You can have a privacy notice even if you're not a covered entity. There's nothing keeping you from complying with HIPAA even if you're not a covered entity. You're just not required to. So if you put together a privacy notice and it was in that notice that that's one of the ways that you're using and disclosing their information. Then that would be appropriate as well without...and then they would just sign that they've received that privacy notice.

Megan: And Val just said, "Good idea, Patty." So thank you for sharing that thought.

Patty: Good.

Megan: And then another question did come in. "If they aren't…if we aren't a covered entity, but we do have a business associate agreement with one that is protected, is that protected under HIPAA?"

Patty: Yes. Then everything goes into place. So a business associate, however, doesn't have to have all the same things in place that the covered entity does. For example, if a participant may not still have the right to modify the record, which is one of the provisions that a covered entity would have. So you need to look at your business associate agreement and see what the covered entity has described, specifically that you need to do, because that agreement should have a lot of detail in it as to how they expect you to treat the protected health information. So, for example, if you have a business associate agreement to actually take over the care of an individual, they're probably gonna include in there that you do have to have all things in place that a covered entity would

have. But if you're just doing a small piece for them and it's care management, and they want that covered under HIPAA, then they would specifically state how they wanted you to use or disclose that data.

Megan: Well, so there's no other questions in the chatbox right now, Patty. As I give these reminders about our next steps and upcoming activities, folks, if you have any more questions, chat them in. We have a few moments. So there's a webinar coming up on October 9th from 3:00 to 4 p.m. Eastern time. It's an, "Ask the Expert," webinar. It's on the fourth trimester, "A New Paradigm for Preventing Maternal Mortality." And that's with Dr. Haywood Brown. He is the immediate past president of ACOG, so he'll be presenting on that webinar. And then we have a series of various, kind of, discussion groups and opportunities for you to get engaged with some of your peers that are serving in the same role. And if this isn't your role and you just know somebody on your team that is either a certified lactation counselor, or a father hetero male involvement coordinator, feel free to share this with them.

The second round of discussion group for both these, the CLCs and the father hetero male involvement coordinators, are happening on October 1, on October 11th, with the CLCs, from 1:00 to 2:30. Sorry for the...it seems like the webinar platform duplicates some of these numbers. So it's 1:00 to 2:30 Eastern, and then the male involvement coordinator, fatherhood discussion group is happening on October 16th. And then the third one for that one is November 20th, from 1:00 to 2:30 p.m. Eastern time. If you're interested in either looping in or getting registered for those, you can just email the Healthy Start inbox, and we'll get you connected with the right people.

This webinar, the slides and the researches that Patty shared, and the recording will be posted to our website following the webinar, and the transcript, and that will all be posted there, so check that out on the website.

So there's no other questions waiting. I wanna thank you, Patty, for taking the time to present on this webinar. And I also wanna thank all of you for taking time out of your busy day to participate on the webinar and join in. If any other follow-up questions come up, feel free to send them our way, and we'll loop through with experts like Patty and try and get you an answer. This concludes the webinar. Please take a moment and respond to the poll at the end, or the survey, to let us know your feedback, but this concludes the webinar, and I hope you have a nice rest of your afternoon.

Patty: Thank you very much.

Megan: Thank you.