

***This unedited transcript of a continued webinar is provided in order to facilitate communication accessibility for the viewer and may not be a totally verbatim record of the proceedings. This transcript may contain errors. Copying or distributing this transcript without the express written consent of continued is strictly prohibited. For any questions, please contact [customerservice@continued.com](mailto:customerservice@continued.com)***

## Current HIPAA Guidelines for Audiology

Recorded Nov 4, 2020

Presenter: Amit Gosalia, AuD

- [Elizabeth] It is absolutely my pleasure to introduce today's presenter Dr. Amit Gos, I can never pronounce your last name. Gosalia is an audiologist at West Valley Hearing Center. He's a board certified, he's board certified by the ABA, a member of ADA, CAA and the Academy of Doctors of Audiology. In addition, he's the co-founder of the AudBoss Private Practice Summit. As a passionate leader for audiology and philanthropy, he's always looking for ways to assist audiologists and students to achieve their goals and today's presentation is part of that. With no further ado, it's over to you, Amit.

- I hope everyone is having a great morning. I'm sure many of you stayed up all night long waiting to find who is going to lead this country in the future. Well, I have some good news and maybe some bad news, we still don't know the answer to that. So forget the red wave and the blue wave. Today we're gonna focus on the HIPAA wave, right? So I wanna spend this next hour and I usually speak a little bit faster when I'm doing these talks virtually versus when we're live so I will do my best to fill the hour here for you guys and of course I believe there's gonna be some Q&A around this process along. So thank you, Elizabeth, for that introduction and I wanna thank aud, for inviting me. Do this, thank you, I'm moving my mic closer here. Is that better guys? Thank you, Margret. Hopefully, thank you guys, okay, perfect. So I won't start over. Let's just keep going here. So I do wanna talk very quickly about what our plan is today. So I'm gonna go over everything to do with HIPAA. I do have these disclosures, so you can read those and of course later on if you wanna really dive into that, you can. The learner outcomes today, I am gonna read these off to you. So number one, after this course participants will be able to identify at least three areas of improvement to be in compliance with HIPAA. Number two, after this course, participants will be able to describe communication methods that are HIPAA compliant. And finally number three, after this course participants will be able to develop appropriate HIPAA forms for their clinics. There's nothing else you're gonna learn except for those three things. I'm kidding, of course we're gonna hopefully learn a lot more than that. So I'm not gonna repeat my history, thank you, Elizabeth, again. I am just a couple of things here,

recently I was the past president of the Audiology Practice Standards Organization. I do work with a lot of students. I do a lot of consulting as well. I think the most relevant point in my background here is the very last one. The very bottom line here. I went through a voluntary audit of my clinics when I was up in Vancouver, Washington where I own two locations. And that was maybe a positive thing. I think the end result was positive, but it was maybe one of the dumber things I've done in my career because I had had asked the wrong people for help.

And I'll explain that in a little bit on who to call and, or maybe who not to call. But the idea is that I actually reached out to an agency, a government agency asking if my clinic was HIPAA compliant. And they came back with hundreds of items that needed to be in compliance. Most of the things that I had done in my clinic, comprised of maybe one fourth of this list and I looked at the list and it was very daunting and I thought, oh boy, I've really screwed up. I need to do all these things, but I'm not gonna do it, 'cause it costs a lot of money to revamp your practices. Well, sure enough, this government agency, a few months later, came and said, we wanna find out if you made those changes. And I thought, oh, great. So we're gonna send somebody out to your office and take a look at your office and make sure you made these changes. Well, the bad news was I had not made the changes so I quickly hired a HIPAA company. They came through, found a bunch of things that needed to be changed and so we made a bunch of those changes. And sure enough a few months later that government agent showed up. It was a quote-unquote voluntary HIPAA audit. It was not voluntary but it ended up being voluntary. I recently did a poll on Facebook in an audiologist Facebook asking people how many people have actually gone through a voluntary HIPAA audit. Out of the 75 respondents, 72 said no and three of us said yes. So it's not something that I recommend, but it is something that you can do if you like to punish yourself. In 2018, the government fined corporations and companies \$28.7 million in fines related to HIPAA. \$28.7 million, now you might think that's a lot of money and some of you might think, ah, that's not that much. That's a lot of money, okay? So I'm gonna jump around with some dates, because I think this is important

first. In October, Anthem, excuse me October 2018, Anthem which is a national insurance company, they paid the largest fine ever for a data breach, not even their fault. There's two ways to look at it. It could be their fault because they didn't have their systems in place that were protecting PHI or protected health information of all their members. However, somebody had hacked in or they had a leak or something happened where there was a data breach and they got fined \$16 million. In November, so that's a big company, right? So Anthem being a national insurance company is a huge company. What about a small private practice like many of us are in? Well, in November, a month later, Allergy Associates of Hartford settled for \$125,000 for releasing protected health information to a reporter. \$125,000, some of us in clinics don't generate that in our salaries, right?

Some of you may say, wow, that's a lot of money. It's a lot money for a small practice to have to pay out \$125,000. So what happened in this situation? A patient went to the news channel. You probably seen those where the news channels will take complaints and they'll go at the business and say, hey, what happened here, kind of a gotcha moment. And they went. They talked to the patient. The patient gave out all the information about what happened, why was it a case that should come to the news's attention. Well, then that channel went Allergy Associates of Hartford and said, hey, Joe Smith or whoever said all these things. Well, Allergy Associates of Hartford wanted to defend themselves and started to say, well, this person had this and this and this and we followed this, this, this protocol. Immediately they violated HIPAA, right? So what happened here is the patient ended up filing a claim, a complaint and they settled \$125,000. I am not in business and neither should you be in business to make money to pay fines, so hopefully by the end of today, you guys will agree with me that we don't wanna pay fines for violating any of these rules. So in 2019 the total fines were 12.274 million. This is from the HIPAA Journal. It's a website. I have a link at the bottom there. They have a lot of information about HIPAA and things that you could look up including some content that might be important for you. But you can see that in 2019 where those penalties came from. You will Touchstone Medical Imaging paying

out \$3 million, University of Rochester \$3 million. These are humongous numbers. Including Elite Dental Associates, so the fourth one down \$10,000. So we just talked about the Allergy Associates, what about a dentist? Well, Elite Dental Associates paid out 10,000 bucks. That's a lot of money as well. And I don't, again, I'm gonna say this multiple times today, I don't want you to spend a dime on any kind of fines, so hopefully when we're done with this you'll understand. But 10,000 bucks for Elite Dental Associates, in a private practice I would never wanna spend again a dollar on fines. So we'll come back to Elite Dental later.

So let's talk about some definitions. I see HIPAA spelled so many different ways. You guys know 'cause the title of this is about HIPAA so hopefully in fact, Audiology Online here on the handouts here actually spelled HIPAA incorrectly. It's H-I-P-A-A, it's the first one and I see that on the left side, the left box. I didn't notice it before, so it's probably my fault. But HIPAA is spelled H-I-P-A-A, not H-I-P-P-A. It's definitely not H-I-P-P-O. Believe it or not I have seen that spelled that way. And of course it's not H-I-P-P-I-E. We do have the HIPAA police, not the hippo police. And of course we do have some folks who are hippies. These are actually some of our colleagues in the industry who were gracious enough to send me their pictures of them being hippies. Some familiar folks: Christina Gram, Douglas Beck, Dave Favre, Dennis Van, I'm not gonna name everybody, fun stuff here. Okay, so let's move on. HIPAA, what does HIPAA stand for? Why is it H-I-P-A-A and not H-I-P-P-A? Because it's the Health Insurance Portability and Accountability Act. We don't see the word privacy anywhere in there. That's why there's only one P. Health Insurance Portability and Accountability Act. It was actually created 23 years ago, 24 years ago by, and signed by President Bill Clinton. The original purpose was actually to help the administrative costs especially while we were starting to trans, transition, excuse me, transition into electronic transmissions of billing. So you can read 'em. I hate reading slides, so I'm not gonna read that out loud, but you can see that the original purpose was not about privacy. In 2013 which was a long time later, there were modifications that were made to HIPAA in accordance with what's called the Health Information Technology for Economic and

Clinical Health Act. That's a lot to say and they actually call that the HITECH Act. The HITECH, I know that in my practice every time I worked with HIPAA I would always hear about HITECH, HITECH and at first I thought HITECH meaning cool hi-tech technology. No, it's HITECH meaning related to HIPAA. The reality here is we started to create what's called Business Associate Agreements. Many of us who work with hearing aid manufacturers, you have signed a Business Associate Agreement, it's called a BAA. If you are billing insurances for your patients, which I'm hoping everybody here is doing, you have signed a BAA or it's been included in the contract with your agreement. Including buying groups, so I've been part of many buying groups in the past, not right now.

However, when you're part of a buying group, you need to have a BAA and most, if not all of them, have that incorporated. I know that I was part of a buying management group years ago and at some point they said, hey, we need these signed immediately, because they realized we had not. Because we're sharing information across, across lines and they're not part of our office, that you're gonna share that PHI, they need to be part of this BAA. In 2010, to go back a couple years, the FTC extended a breach notification rule and they started to enforce some of these HIPAA violations. So of course electronic health records were not readily available back in 70s, 80s, not so much in the 90s, but in the 2000s and now of course. So OCR undertook its first round of HIPAA audits in healthcare organizations of 2012 and 2013. What is OCR? OCR, hold on, let's do this right. OCR is our HIPAA police, okay? This is my friend David DeKriek who's down here in Los Angeles. We were at a conference and he showed up to show this, he wore this shirt in my, just for me, which is very nice. But OCR is the Office of Civil Rights. Okay so the Office of Civil Rights is who monitors and polices HIPAA violations. So let's go back. When I told that I contacted a government agency, I contacted the Health and Human Services and they told me to contact the Office of Civil Rights. Now when I read the name Office of Civil Rights, it took me back for a moment. I thought, wait a second, I'm not looking for a civil rights issue, I'm looking for a government medical healthcare privacy issue. Well, sure enough, OCR is who polices

it. That's the division of the Health and Human Services that polices HIPAA violations. Now that might be a negative thing, okay? So whichever way you look at it, if it's negative or positive, that's either here nor there. But they also provide training and materials. You could look up your state's Health and Human Services website and within there you will find a link to the Office of Civil Rights or anytime you type for example California HIPAA, there is a link that will take me to California's Office of Civil Rights.

So I think I've hit the first one here, why is it important to follow HIPAA? Well, as I mentioned in the beginning and I mentioned a couple of times already, why pay fines? We don't wanna pay fines. So follow HIPAA for the main purpose of not paying fines. If you wanna pay fines and you feel like spending money, send the money to me. I'm more than happy to take your money. But don't send it to the government because you didn't follow some simple guidelines. But you need to follow HIPAA or the privacy laws if you are a covered entity. So what's a covered entity? A covered entity is somebody who works with health insurances, clearinghouses, or you're sending any electronically transmitted information in connection with transactions for which they've adopted these standards for. So that's kind of the legalize way of explaining that if you're gonna send any information about a patient electronically, you are now a covered entity. So most of us who bill insurance companies, the reason why I keep saying most of us, because there are audiologists who don't, they've opted out. They don't bill any insurance companies.

So theoretically there is a case to be made that if you were not billing insurance companies, maybe, maybe, and as long as you're not transmitting information electronically, maybe you don't fall under this umbrella of a covered entity. Now why do I say maybe? There's no definitive answer. Most insurance companies will have in their contracts that if you're gonna work with us, then you're gonna abide by HIPAA, but if you're not working with an insurance company, then you have to decide does your state law require that you follow privacy laws. It's probably just good practice

anyways. PHI, I've mentioned it a couple of times, and again PHI does not say privacy. A lot of people say, oh, I have private health information or patient health information. That's not correct. It's actually protected health information. And the reason why it's protected health information is because there's a bunch of information that is under that umbrella of what is considered protected health information. Well, it can be demographic data. So here in private practice, again, we look at demographic data when we do mailers for example. So that demographic information is considered protected health information. What about medical histories, okay?

So any patient that you see, they've got a medical history. I can't go talk to my buddy and say, oh, yeah, Steve over there, yeah, he's got a disease. I can't do that. That's protected health information. Test results, can't share test results. Insurance information, I can't tell Jane that Joe has medical or Blue Cross. Information used to identify a patient or provide healthcare services or healthcare coverage. So any of that information is called protected health information. That is what you need to protect. Here are more things that are considered protected information. Of course, names. I can't go out and say Joe Smith was here, right? That's Joe Smith's name. Sure, Joe Smith's a common name. However, I can't say that. All geographic, I'm not gonna read that, but all geographic identifiers. I mean, basically, you can't state that somebody from this specific area was in your office. Pretty crazy, so that's a big one right there. Dates or something related to an individual. Hey, yeah, I just saw this patient yesterday. He just walked out the door. Oh, I saw that guy walk out. That's protected health information. Obviously phone numbers, fax numbers, email addresses, social security numbers, of course social security numbers, and medical record numbers. So yesterday I received an email. We work with a insurance company here called Kaiser. I know it's not all around the country. But they send us patients. We're one of the only clinics that get outside patients from Kaiser. However, they had a question for me. They sent me an email and the email was so generic in the sense that, hey, medical record number 4-0-blah-blah-blah-blah-blah, whatever the number, it wasn't 4-0, just in case anyone was thinking I just gave out two numbers of the medical number. But it

was this long medical record number and I have no idea who that patient is, because the medical record number was Kaiser's medical record, not my, or our medical record number. Now even though it was a secure email that they sent to me, they still, even after I asked 'em, I said can you tell me what date they were set here so I could look up the patient. Can't do it. They could. But they decided that they couldn't do it. So now we're at a standstill. Now we have to go back and look through all of our referrals from the last six months, we're assuming, 'cause he wouldn't even tell me when the patient was in to find that medical record number so we could answer the question. That's how strict you can be versus lenient. Now this seems like a lot of information, protected health information. But wait, there's more.

So health insurance beneficiary numbers, account numbers, license numbers, vehicle identifiers. I can't say, oh, did you see that patient's license plate? That was awesome. It said whatever. That's protected health information. URLs I don't quite understand. I've looked up many times, but I can't even give out their websites, which of course I wouldn't do. IP addresses, I personally don't know how to find that on somebody anyways. Biometric identifiers, if I end up taking a fingerprint scan of somebody, I can't share that with, let's say Elizabeth Thompson says, hey, I have a friend and they were in your office. Can you send me their thumb print? I don't know why she would ask me that, but I can't share that either. Including retinal, I don't know if you guys are doing retinal scans, we're not of course, voice prints. Even photographs of patients. So any comparable, anything to do with that patient, anything at all, you can't really share that information unless you have a BAA signed with somebody and they're covered and you guys are both covered entities. Pretty darn strict, okay? So lets have a little break here. I live in Los Angeles. And here we have the world champion Los Angeles Lakers who just won the basketball championship. And please know that it hurts me to say that, because I'm not a Lakers fan, but I live in Los Angeles and everyone around me is a huge Lakers fan, so I'm gonna use them as my, the burnt of our question here. So Anthony Davis who, if you're not familiar with basketball, he's one of the best basketball players out there, refers his teammate LeBron James, who by the way is

probably the best basketball player out there. He refers his teammate LeBron James for a hearing test. Because when Anthony Davis yells at LeBron James to pass the ball, LeBron doesn't hear him all the time and rarely ever passes the ball. One month later you run into Anthony Davis and he asks you, hey, did LeBron actually come in and does he truly have a hearing loss? What would you do?

So here are your three answers and I believe we have a poll, so you guys get to answer this. This is a fun interactive here. See if you guys are paying attention. Answer A, get a autograph and spill the beans. I'm sure that autograph would be worth so much money. You could pay that fee, that fine with the money you get from that autograph. Well, probably not. B, tell him that LeBron has normal hearing, he's just a ball-hog and guess what? You're never gonna win another championship and I would love to be the person to tell him that. Or C, disclose that due to privacy reasons, you cannot disclose that information. I know this is a tough, tough, tough question. I see 46 responses so far, 47 responses. I know that's a little bit less than, a little bit close to half of the people out there.

Well, I think you guys know what the answer is, so I'm gonna go forward and I'm gonna go ahead and tell you. If you were the two people who chose A, I'm sorry, please boot those people from the class or make 'em stay after for a little one-on-one session. The answer is C, disclose that due to privacy reasons, you cannot disclose that information. Now being in Los Angeles, we get a lot of celebrity patients and they refer their friends, music bands, rock stars, if you will, from the 90s and 80s who now are in their 60s and 70s and they refer their band mates and of course they wanna know how it went. Can't tell you. I can't tell you. So I would say, you know what? Unfortunately because of HIPAA, I can't tell you that information. Well, at least did he come in? I can't tell you that information. I have to be that strict. As much as I'd love them them that, yes, they came in. I can't tell 'em. So as audiologists, as health care providers, what do we need to do? So I said this earlier, we have to protect our patient's protected health information. I recommend and I know that there's different

ways that different audiologists, different practices do this, I recommend you have your patients sign a HIPAA release or a compliance form. Now I'll put a little asterisk mark there because there is a caveat to this. But in our office, if the patient does not sign the privacy, excuse me, the HIPAA release or compliance form, we have a very firm policy that we will not see that patient and the reason why is because then we cannot build that patient's insurance. Right, so if a patient comes in for an audio, because they have a hearing loss and they come in and they say, you know what? I don't wanna sign this. That means they have the wrong idea that they're gonna sign this and that allows me to sell their information which is not what it is. What it really does, it protects the patient from us selling their information.

Now naturally we're a covered entity. We would never sell their information, but this is the image that a lot of patients have. We have patients who don't wanna give us their driver's license because they think that we're gonna take that information and either we're gonna sell it or someone's gonna hack into our systems and steal that information. Hopefully that never happens, but that's the mentality that a lot of people have. They're worried that their information is gonna get stolen or shared. Well, that compliance form protects them and we use that information to build their insurance companies. Even our veterans who come in from the VA who are part of a community care program or whatever it's called these days, the community care program, we get these veterans who come in, well, we need their social security number. Think how many people really wanna give up their social security number? Not many, so luckily the last four digits is all we need and it's usually on the referral forms that we get. However, we still want them to sign a compliance form. That compliance form has a bunch of information written on it. I failed to share that here, I apologize. I wanted to put the wording on here and I, months ago, I totally forgot to do that, but the reality is you could look up sample compliance forms. I'll have my contact info at the end of this seminar. If you want to email me, I'm more than happy to share what we developed which covers just about everything that you need to cover. A signed HIPAA release form must be obtained from a patient before their PHI can be shared, okay? Now what

is the caveat? The caveat is you can have them sign another form. And the other form is that, you know what? This is going to be a kind of a waver, call it HIPAA waver. So you're getting them to sign something and so now you give them this other form. We don't have one of those. We, our office, we just don't believe in that. We wanna follow these guidelines, 'cause of course we don't want the audits. But you can have a form that says, I so and so wave my privacy or my HIPAA rights or whatever you wanna call it. I don't even wanna know what the language, but you can have that and now the patient might look at that and say, wait a second, I don't wanna wave my rights. Sure, then sign the compliance form saying that we're gonna do our job to protect your information. And I know because I'm part of numerous groups and a lot of times we find, we find that people will use these waver forms. There's a question that popped up, it's very timely, how often, I can read the whole question but how often do you have them sign it, I believe is the question.

I hope that's the full question, 'cause I can only see how often do you AHA. I will actually have them do it once a calender year. There are numerous different ways to do it. We find, and the research I've done, generally states that once a calender year is appropriate. Now it's always fun when I see somebody December 27th and then they come in January 4th for a followup. Yeah, we need another one to sign, but you won't have to sign it again for the rest of this year. I know some people say, yeah, but they were just here, right? But if you follow, once you set that protocol in place and if you say calender year, I don't care if they come December 31st and January 1st, make 'em sign it twice. Say, you know what? You've just signed this the other day. We have to do it every calender year. Communication, I know we all have masters or doctorates in communication disorders, but let's be more proactive in communication where we tell the patient exactly why they're signing this form, what they're signing and why it's important for them. And why we're doing it again even just a week later. Right now, I know this is a little off topic, but right now with COVID-19, every single time a patient walks in, we have 'em sign our COVID form. I don't even know what we call it, COVID questionnaire. Patient comes in yesterday, they come in today, they're signing it again,

okay? That's how strict at least we are. And nobody, people might say something about it, it's not a big deal. The reality is they all sign it. They all fill it out. We actually even have a little curve ball question in there so they don't just circle yes on all the questions. They need write no on one or circle no on one of them. So with the HIPAA stuff, it's not that difficult once you start to explain and once your staff and your teams understand why they have to fill out this form. Why it's important for the patient. Patients will sign it every single time. Margret, I, let me see if I click on that, there we go. Can you explain please, except in the case of routine disclosures, et cetera, on the slide? Let's see, a signed HIPAA release form. Thank you, Margret. A signed HIPAA release form must be obtained from a patient before the PHI can be shared with other individuals or except in the case of routine disclosures for treatment, payment or healthcare operations.

So this was a paragraph that was taken specifically from the OCR website. And the idea here is when you have certain disclosures that you are not going to share their information and you have ongoing treatment, this is where someone's coming in for a followup on treatment, that you don't have to have them come in or sign the form multiple times. So I use it again once every calendar year, so again even if their treatment plan spans past December 31st, we're still gonna have 'em sign it once again. But in theory, you don't have to have 'em sign it every single time. Ada, let me see, we don't dispense hearing aids, so patient's requests that we fax the audiogram to their audiologist dispensers. Do we need to have a HIPAA release form? This is a great question. This is definitely something that's come up a lot recently. In fact there is, sorry, I keep bringing up Facebook and social media but that's where we do a lot of our information sharing. Somebody just recently said that, you know know what? A patient wanted me to come in, do the audio, send the results back. Well, we are all health care professionals and the reality is once the patient signs a HIPAA privacy compliance form with your office, you are allowed to share it with other health care providers as long as there's a referring agreement. One potential way to protect yourself, have that other clinic sign a Business Associate Agreement. So use this with

anybody. We sometimes go, we used to, and we kinda lightened up a little bit, we used to ask the patient to sign a information release form even when we were sending reports back to physicians. We've stopped doing that, because we don't need to do that. So physicians versus audiologists versus chiropractors versus dentists, the reality is we're all part of, we're all covered entities. As long as they're part of the referral process that has regarded the patient's care, you can actually send that without a release form to that other provider.

So this becomes a little sticky if the provider, which happens often, I get, I'm sure you all do as well, we get referrals from colleagues. And they say, hey, this was, I'm sending my mom to you 'cause they live pretty close to you. How'd it go? Well, your mom didn't say that we could tell you. So on our HIPAA compliance form, one of the things that we have written on the questionnaire, if you will, is who can we share your information with? And if it's a spouse, we ask 'em to write their spouse's name. Children, write the children's names. Believe it or not, it happens all the time, the person has three kids but they only want two of them to be involved in their care. We can't talk to that third one. We can't tell that third kid what happened. So same thing, if an audiologist sends a patient to me and it's a relative, in theory, because it's not regarding continual care, I really can't unless, don't get me wrong. Sometimes we'll tell the patient, hey, do you want us to be able to talk to your child or whoever that audiologist is. Can we get you to write their name on the compliance form because sometimes patients don't understand that sentence or that line. So it is important. I'm gonna quickly answer these questions here so as we go along. Rebecca Dillon asked, "Can you only share that one time "with a referral or in future as well? "Say a test is a year later within the same calender year." Yes, Rebecca, so again if it's related to the care, the health care of the patient, if that referring physician or provider is requesting another copy, yes, absolutely, you can send it over and over again. Because even though we don't have a BAA, sorry, I didn't mean to do that in quotes. Even though we don't have a BAA with that physician, we don't need one because we're still covered under the health care providers covered entity program. So Donna King asked, "Do we

need Business Associate Agreement "with our database provider?" You probably have already signed one. So CounselEAR, TIMS, HearForm, Sycle, they all have Business Associate Agreements, because now you're restoring, that's probably the biggest PHI information that somebody else could have. So I know for a fact that, well, I should say that I know almost for a fact that each of these OMS systems or database providers have Business Associate Agreements signed by you. Sometimes it's written into the contract where you're signing up with them, so it is in there. Stacy Moore, hi, Stacy. Accepting the case of routine disclosures means that the form was already signed. So generally speaking, I interpret this as, you know what? We have a compliance form signed by the patient and we're gonna be doing continual care.

So again because we used this on a calendar year, if you decide you don't wanna do it on a calendar and you wanna do it from one year from when the patient first came in, you can do that as well. I think it's a little bit harder to manage that. But if you say one year from the date they signed it, now I'm gonna have 'em sign it. So let's say November 4th today, November 4th next year they need to sign another one. Well, during that period, you don't have 'em to keep, I'm sorry, Elizabeth, yeah, I'll do that. The continual care over the span of the year, you don't need to have them continually sign a new compliance form. I hope that answers that. I know that's a little sticky and even internally here we are, we're a little bit stricter, I think, okay? And I say that only because I've gone through this process and I don't wanna go through it again. I'm not trying to scare you. They're not peeping in your windows and looking at what you're doing. However, once you've gone through it, you're a little bit more apprehensive on the forms and compliance forms that you need. Rebecca, let's see here, if the patient requests us to send results to primary care but we don't have a referral from them, is that okay as well or should that doctor be put on the HIPAA form? That's a good question. As long as it's part of the patient's continual care and it's their primary care physician, no problem. You do not need a business associate, a Business Associate Agreement with that primary care physician, you can send the results. If you want to be very, very safe, have them sign a release form or, yes, you can ask them to put the

physician's name or whatever they wanna put down on that line where it says share my information with so and so. It's not needed. So again, as long as everyone's a covered entity, which most physicians, and I don't have this down as a fact. However, I believe most physicians have to comply with HIPAA. Whether they're concierge medicine or not. With audiologists and dentists and or the, I've lost the term out of my head, but the rest of us, we are kind of in this gray area. So you don't have to have them listed, you also don't need to have them sign a release form. Margret, what if they have a referral from their primary care and then later we want to send information results to an ENT? Does the patient have to sign again with the ENT name? No, you don't.

So again because we're all part of the same umbrella, if you will, of health care, you can send those results to the ear, nose and throat. Of course there is a point where you have to decide, do I wanna be proactive and send the report to a otolaryngologist before the patient even calls the otolaryngologists? What we do, this is just us, we will ask the patient, make the appointment, call us after you've done it, let us know who you decided to go to and then we're gonna send your report to that place. That way everyone's on the same page. We have two otolaryngologists here locally that we like. We send referrals to them when we can. However, if the patient decides not to go there and go somewhere, now we just sent information over, it's still okay to do that. However, the patient may say, no, I didn't want it to go there and now you've created a potential appearance of a violation of HIPAA even though it's not, okay? So let's be very clear, you can send reports to any medical professional that's involved in care, but if you wanna be safe, make sure the patient is at least involved with that professional first and then go through it and send those, that information. Dixie, I thought that initially faxes were not considered electronic transmission. Yeah, so faxes, our biggest faxes can get hacked and that's something I didn't know. So there are ways that faxes can get hacked. So now especially with e-faxes that are goin' on, there is a potential for faxes to be considered electronic transmission as well. Susan, in regards to educational audiologists working with clinical audiologist, we both work providing continual care to the child. Do we need to have the parents to sign a release of

information form to obtain audiologic data from the private clinical audiologist? The answer is no. So according to the Privacy Act and the HIPAA rules, the answer is no. I recommend it. So I like to be a little bit safer. It doesn't hurt anybody. If anything, it just protects everybody involved. So the short answer to Susan's question here is get the signature, but you don't need it. So if you're not doing it now and you don't wanna do it, you should be fine. Next slide, all right. So what is your, I'm gonna move on. And of course keep asking questions, guys. I'm more than happy to keep jumping in and answering questions that our team here from Audiology Online are doing a great job of clearing out the questions so I'm not getting inundated.

So let's talk about what that HIPAA form should look like. And I keep calling it HIPAA form. Here I wrote release form. Actually on our form it says HIPAA compliance form. Doesn't matter, whatever term you wanna use, their semantics, it's essentially the same. But the release or compliance form basically is a description of the information that we're gonna use. So it tells the patient, you know what? We're gonna take your name, date of birth, insurance ID number, things like that, and we're gonna submit that to a clearinghouse. So earlier I said the word clearinghouse and some of you that are not involved with billing insurance may not know what it means. Well, I don't just send a bill directly to Blue Cross. Usually there's somebody in the middle. The middle organization is called a clearinghouse. Well, if I'm gonna send somebody to a clearinghouse, well, they're usually, no, I shouldn't even say that, they always are following HIPAA guidelines, because they get that information. They're part of the insurance world. They better be part of this. The purpose for which the information will be disclosed. So of course if we're building their insurance, we wanna make sure that the patient understands that we're using their information to submit to their insurance company so we can get paid for our time. It's a novel concept to get paid for our time. The name of the person or entity with who the information will be disclosed. So on there, we don't identify, in this example that I used, we're not gonna identify Blue Cross Blue Shield. We generally will say clearinghouse, insurance company, we use more generic terms. We wanna use an expiration date. Generally we wanna say

something to the effect that this contract will expire 12 months from today's date. Which is what we have because we have them sign it every year. You could have it six months. You could have it every two years. The recommended guideline is 12 months. But again, nobody is really checking that and I wanna be very careful about, that I recommend once a year, okay? And again, it's very easy if you do it January 1st onwards. Then every patient that comes on after January 1st and in your OMS you should have an ability to put in a date that they signed it, so during the check-in process, your staff could or your staff could quickly look at. And if they signed it on this date, I don't have to have 'em sign it again 'cause they just signed it on January 1st. Next the signature and date that the authorization is signed by an individual and-or an individual's representative. Now we do get patients who come with a caregiver or what's it called? A legal authority, a power of attorney.

So we have children or friends or somebody who is a power of attorney. They come in, they're the one signing the form. You need to make that very clear on that form that the person signing the form, just 'cause it's a kid of a patient, doesn't mean that that's a legal document. I don't care if the signature looks like a scribble, it doesn't make sense, the patient needs to sign that form unless you have a legal document that the person signing the form is a legally declared power of attorney, okay? So be very careful on that. Sometime we, and I'm guilty as well, me as in our clinic is guilty as well, but sometimes the patient's child will call and say, you know what? They can't sign it. We'll just sign it. And then we don't realize until later that, oh, wait, that person's not even a power of attorney. And then when they sign their, when they're hearing is they end up signing it and, yeah, it might be sloppy, but they signed it, so I'm covered. Emails, so let's switch gears. So I'm sorry. Let me go back one slide. This is basically, this is what needs to be on that release form. What I talked about a couple slides back was I also want to make sure that we put on there who we can share the information with. I also like to have, do you allow us to email you or would you like us text you or you allow us to text you or you allow us to leave messages on your voicemail. Does that sound crazy that leaving messages on a voicemail? So if I call Eliza, I'm gonna

keeping picking on you, Elizabeth. So I'm gonna call Elizabeth. She's my patient, okay? I just violated a HIPAA violation right there. Just kidding. She's not my patient. The idea is let's say she was patient. Now I'm gonna call her and she has a general answering machine and it does not say you've reached Elizabeth's home or you've reached, excuse me, Elizabeth's phone, leave a message. If it just says, the recording says, please leave a message after the beep and it does not say whose phone number that is, you better not leave a message with any PHI. If I leave a message on that general answering machine and I say, hey, Elizabeth Thompson. This is Dr. Gosalia's office and we're calling to let you know that your hearing aids are in for your fitting next week. And now somebody else hears that message, you're in big trouble.

So we make it very clear to our patients that if you don't have a custom voicemail setup that says, this is Elizabeth Thompson's phone. Please leave a message. We as a team, will not leave a message. We'll actually hang up and try to call them again and try to get 'em on the phone. Now that seems pretty ridiculous and it is. However, you can imagine the other side of it if somebody else picked it up and said, what? Why is my mom going to get hearing aids here when I told her to go somewhere else and blah-blah-blah, but the mom didn't like that person or whatever. It could cause all kinds of problems and now we're the culprit. We have to take responsibility. So the accountability rests on us. So be very careful with leaving voicemails. If you do leave a voicemail on a generic mailbox like I said, you can just say hi, this is West Valley Hearing Center. Please give us a call back. And even that is a little tricky because you are disclosing your name which sometimes can lead to somebody saying, oh, West Valley Hearing Center. That means they're going in for something related to hearing. That could be a little tricky. So be safe. I'd rather you be safe than sorry. Emails, so emails has been a very sticky thing. We all wanna email our patients. I email patients periodically. However, when you're emailing a patient and I'm gonna include one example here in a moment. When you're emailing patients, you wanna be as generic as possible if you are not using a secure email system. I'm not here to advertise nor do I have a relationship with any online email HIPAA complying email services. However,

you have the ability via some of the OMS systems. So we use CounselEAR, okay? So again I'm not here representing CounselEAR, but we use CounselEAR and we will communicate with our patients using the CounselEAR encrypted email system. So that way when a patient gets it, there's a way that they could read it. Now there are other companies you can pay for services. We used to use one called protected trust. It's expensive, but it's less expensive than paying out a fine.

So let me explain something or excuse me, let me give you these examples. So back in, I can't remember what year it was, 2014-2015, but somewhere around this audit time. One of our staff members who was just, sorry, she was terrible. So she was emailing patients from her Gmail. We didn't know that. So she had emailed four patients with information about their appointments from her personal Gmail. This is not right. Of course we would, if we knew that, we would've told her immediately, you cannot even open your Gmail in our office. It's part of our policies. When you're on your break, you could use your phone or your laptop, whatever, but not on our clinic computers. You can't open up your Gmail. Well, guess what happened? Somebody, somehow her password got reset. Now we don't know what happened with her password. Did somebody try to hack her account and change her password? Did she nefarious that we didn't know 'cause she didn't like working with us? We don't know.

But because there was a potential hack, we had to go through every single email that she had, which was pretty funny. Went through all of her emails through her personal Gmail and we luckily found those four patients whose information was in those emails. And we contacted each of those patients and we said, listen, we realized that you were emailed from a non-secure email system and the password got reset. There's a potential violation and a potential data breach. We would like to pay for one year of credit servicing, credit monitoring for you. That's like 80 or 90 bucks, I can't remember how much it was. And if you are okay with that, please sign the form in the attachment and send it back to us and we'll send you all the details. Now you can imagine on my earlier slide, Anthem had to pay out \$16 million in fines. They don't just have four

patients. They have millions of patients. So imagine having to pay for credit monitoring for all off those individuals' informations that were breached. So something as simple as that is crucial. So even though we have them sign on their compliance form that they will allow us to email them, we're still gonna take it one step further and only use a secure email system. Office 365, if you're using Outlook, there are some features there. You have to pay, I think you have to pay to be part of that program. But there is a HIPAA complied version of Outlook. You've probably received emails from your care providers, healthcare providers where they say when you log in, you gotta put in a password. When I talked about that Kaiser email, they sent me the email, I saw the email, I clicked a button. It opened up another window that said, we just sent you a code. I had to go back to my email, take that code, punch it in. Now I'm in their secure portal to read their emails.

Otherwise really they can't do that. I'm a patient UCLA at the UCLA Medical system. If I want a message, I just get an email on my personal Gmail that says, you have a message from, or you have an updated message on your UCLA account. I have to log in to my UCLA account, so that's password protected, I log in and then there's all the messages. So those systems of course, Kaiser, Anthem, UCLA, they're humongous organizations. They have money to spend on systems where you can do that. However, there are some more budget friendly systems available. I'm gonna go faster here. Sorry, guys, we're at 13 minutes left. Texting, again, HIPAA still doesn't have a very solid answer about texting. However, if you're an iPhone user, I'm a heavy iPhone user. I do a lot of texting. Apple stores every single text that I sent. So you have to realize that if you're using iMessage on Apple on your iPhones, Apple actually houses that data. So you could imagine if I'm emailing one of our patients, or excuse me, I'm sorry. If I'm texting one of my patients and I'm using my iPhone, that information is stored somewhere. I don't have a BAA with Apple. I can try to send them one. I guarantee they won't sign it. So the reality is you can't really text. Now we also work, again, I'm not advertising them, but we work with a company called MedPB. One of my friends Kevin St. Clergy has created a text system so we can actually go log into that

portal and then we can send text. Of course patients want us to text them. We can't just send a text from our phones. We will use these platforms. You could look it up. HIPAA compliant text platforms. But most texts are not HIPAA compliant, so be very, very careful with that. Oh, also, if you're sending an iMessage, again, I'm using Apple, 'cause I'm a big Apple guy, if you're using iMessage, it is using the internet, so you do end up using Wi-Fi networks and if those Wi-Fi networks are not secure, you're in trouble again. What about online reviews? So this is another topic that we talk about quite a bit. Somebody goes on. They give you an online review. How do you respond? Well, do you respond, number one? Of course. Always respond. I always recommend you respond. That's a whole different topic. But always respond, but you wanna be as generic as possible.

In fact I recommend you don't focus on the patient's situation, why they were in your office. Focus on your office protocols and policies. If somebody says, oh, when I went in, I got my hearing aids from Dr. Gosalia. Well, don't go in and say, yeah, we chose the best hearing aids. Say, we appreciate the compliment. We strive to provide the best service to everybody. Or something very generic like that. So here's some examples. This was one. This is not mine. I wish it was. I could not speak more highly of this clinic. They treated my injury with a proper sense of urgency and compassion warranted. They were very sensitive to my needs and accommodated my requests happily. I really felt important and cared for, blah-blah-blah, I don't even know the rest. The response from the owner. Thank you so much for your review. This means so much to us, because we strive to make everyone feel better faster without the headaches of accessing care. This is a, the green check mark indicates this is a good way to respond, okay? What's the opposite of a green check mark? A red X. I had some pain in my back and I had a walk-in appointment with Dr. so and so and she was so thorough and patient. I definitely recommend both her and this clinic. This is a great review. And the clinic responded, but remember, red X. Thanks Mr. so and so. I'm happy you had a great experience and glad I could help you manage your scoliosis pain. No. Don't do that. You can't sell, you cannot put it on here. I don't care that the

patient wrote it and you shouldn't care either. They can write whatever they want. We are the covered entity and we cannot indicate that this patient has scoliosis pain. Which I don't think I've ever made that comment to any patient of course, but the reality is think about it in our four wall. So remember Elite Dental Associates I talked about earlier? 10,000 bucks they had to pay in fines. Well, what happened here? They responded to a review on Yelp. I don't have a copy. The review is gone. I think probably 'cause they were fined for it and they had it removed. They had a Yelp review where they responded disclosing PHI based on the procedure that that patient had. It was nothing negative. It was a positive review. Of course you're happy you got this positive review. You wanna say, yes. We choose the best crowns or the best whatever for your needs. Well, yeah, but now you just violated and unfortunately they were caught and that's what happened. Well, here's one that we had and of course, I love this one because I want to show you more real world in our four wall, if you will. I'm not gonna read this, but essentially he gave us a positive review. Okay, he was a very tough patient. He's a very funny guy.

In fact I covered his name up, but he signed all the releases. We could share his information. But still I don't wanna do that. So even right now I asked him and he signed a form that I can use this picture. This is from his camera, not mine. He wanted to take the selfie, 'cause he was so happy. I digress, let's move on. This was our response. Thank you for your kind words. We strive to provide the best care possible for all of our patients. So here he's indicated that he came in, got it done. Everyone knows he's a patient. We did not talk about what's going on with his ears. We didn't talk about what we did. We didn't mention that he questions. We didn't mention that whatever was up here that would violate any rules with HIPAA, okay? Okay, this is very current. And it's kind of, I don't wanna point fun at anybody. That's not the purpose here. When you are on some of our audiology social media pages, okay, I know that there are some big ones. We share a lot of information. We share information about cases. We share information about patients. Always remember if you're gonna share a case, okay? So we see audiograms posted. There was one this morning, okay? So

somebody posted an audiogram. Of course, covered their name, right? Covered the date of birth, covered any identifying information. So I've done this, but I will screenshot or crop just the audiogram, right? So I don't have the patient's name. I don't have the date of birth. I don't have anything that identifies who that patient may have been. And then I can post it. Now if just post the audiogram, I don't need to say I have permission from my patient that I could post her audiogram, because I didn't put any of that patient's information in there. If I have a picture of their ear, it's impossible for someone to say that belongs to so and so unless somebody has a tattoo or a specific earring that identifies somebody.

Let's say, I can't even think about it, but let's say there's a musician or somebody, a celebrity who has a specific thing with their ear and everybody knows it. Well, then if you're gonna share that picture because that person came to your office, then you need to get that patient's permission. However, you don't need to tell us. I don't need to know that you got your patient's permission. Makes no difference to me or you whether or not you got your patient's permission. You know who it makes a difference to, your patient. Your patient, if they find out, wait a second, they just shared my information online on a social media page and I didn't give 'em permission and they had my name in there. Now there's a bigger problem. But if I share a patient's information and they've signed off on it, you don't need to know that I got the patient's information because the courts don't care if you write I got my patient's permission. The courts care if you did get your patient's permission, but they don't care if you write that.

So this was something that happened recently. This is a brand new slide I just threw in just in the last two weeks because it just came up. It was more of a joke, but then it became very serious, because people were starting to debate. No, you need to write you have the patient, no you don't, you don't. So the final answer is protect your patient's information to the best of your abilities. Don't share information if you don't have their consent, okay? I don't have a summary slide. I just have my Q&A and

contact info. But protect your patients and that's patients being plural. Your patients' information. I've gone over all the information that you gotta protect. But be as safe, I'd rather you're more safer than sorry, because OCR is not a organization that any of us wanna mess with. They're very trigger happy in terms of fining. So be careful. But it's not hard as you can tell. Just use the right forms and again, thank you so much for listening after spending all night watching the red wave and the blue wave. So there's my contact info of course. You can email me. You can reach out to me. Yes. Thank you.

- [Elizabeth] Very good. Thank you so much, Amit, for a fantastic presentation. Any questions come in, I'll kind of ad lib here for a few moments while we see if any questions, any last minute questions come in. One question I had was when you're talking about gaining permission for patients to share information whether it be in a journal, if you're gonna do a journal submission or on social media to give advice from other colleagues. Do you do more of a blanket release for them or are you pretty specific about how you're gonna share that information?

- So I hear this question quite a bit. So what we use, because we get a lot of, again, I'm not, I say this and I'm sorry, it sounds like I'm gloating. But we get a lot of celebrities that come in and of course we wanna share, because we're very involved with audiology awareness. We have a separate photo and video release form that we use. And it's totally separate where if I get a picture with somebody or they get a picture in the office, getting impressions taken, I'll have them sign that photo release, sorry, photo and video release form, 'cause we do get some that will share videos. And if you've seen some of my videos, you know who some of those celebrities are. But the reality is that form itself is a more blanket form that I can do anything with that information. Once they sign it, I can say that they were here which I don't really wanna do. But I can say that they were here. I can share pictures of them. I can share their videos and I can do it almost anywhere, because my form states that we can do that almost anywhere. I highly recommend if you're gonna develop your own form, I

recommend you have your business attorney review it, because every state's just a little different. But the bottom line is once you have that document in place, you can use it anywhere. And I've worked with AAA on many tasks and our form is surprisingly very similar to AAA's photo and video release form. So it is something that it is more of a blanket statement. Does that answer your question, Elizabeth?

- [Elizabeth] Yeah, I think it's really good advice to have as we do promotion and hopefully all of us that are practicing audiology are promoting the good work that we are doing with our patients. That's one of the things that we all need to collectively do is to get the word out about how audiology can make a difference in people's lives and so, but having that protection for the practice too around what making sure that the consumer knows exactly what information's gonna get shared. One question came in. I'm assuming the heardr@gmail.com is the best email to grab for you if you'd like, if anybody has questions or further questions or to share, maybe get a sample of your HIPAA release form or BAA form-

- You gotta stay after, 'cause you spelled HIPAA wrong. I'm very sticky about that.

- Well with that-

- I just, you're gonna write HIPAA a hundred times on the whiteboard. I'm just kidding. So, yeah, the heardr, heardoctor@gmail is perfect. You're not sending me any private information. So that's absolutely fine.

- [Elizabeth] Well, thank you so much for an incredible course. And I feel like we all feel a little smarter today and all know how to spell HIPAA now. So thank you so much Dr. Gosalia for your time and expertise. Thanks for everybody for participating today. And we look forward to your feedback on this course and also future courses on Audiology Online. Thanks so much. Buh-bye.