

Title: HIPAA Compliance Lessons and Breaches in 2022

Date & Time: January 27, 2022 at 1pm ET

APA/Robin Tiberio: Hello, everyone. Welcome to today's webinar, HIPAA Compliance Lessons and Breaches in 2022. This webinar is paid for by Compliancy Group, APA's preferred provider for HIPAA compliance solutions. Some important points before we get started. APA does not endorse any products or services. The content was created by Compliancy Group and does not reflect the views of APA or its editorial staff. You can email advertising@apa.org if you'd like to learn more. This program does not offer CE, however, we will email everyone watching live today a certificate of attendance. Certificates will only be issued to those who watch for a minimum of 45 minutes.

We will be recording this presentation, and it will be emailed to everyone in about two weeks' time. That email will also include a copy of the presentation slides. During our time together, you will be on mute. You can communicate with us using the Q&A box located on your webinar screen. If you have a question for our presenter, please type them in using that Q&A box. A link to the presentation slides will also be posted in the chat box on your webinar screen. If you miss it, we will email those slides along with the recording.

With that, I would like to introduce today's presenter, Liam Degnan. Liam has an eight-plus-year history of experience, combining risk management, software as a service sales, and regulatory compliance in the healthcare space. As Compliancy Group's Director of Strategic Initiatives, he advises healthcare decision-makers, behavioral health providers, and medical vendors. He speaks on a variety of platforms and topics with an emphasis on simplifying complex HIPAA regulations. Welcome, Liam.

Liam Degnan: Thank you all for having me. Much appreciated. I'll say, as we get into this for today, folks, the general framework that we're going to follow with the content of the webinar today is really two or three things. We want to make this as practical as possible as far as taking some of what HIPAA requires, but really looking at some real-world case studies, things that have been happening in the last year, ways that things can potentially go wrong, and then also reviewing generally what you need for a HIPAA compliance program and some key takeaways that you can be bringing back to your practice to simplify and make the whole management of your HIPAA compliance requirements a little bit easier.

We're going to start just by laying a general framework and a foundation as far as HIPAA compliance is concerned. One thing I will say is if you are coming to this webinar with specific questions, I know a bunch of you sent questions in ahead of time, but as I'm going through some of these topics, if there are things that are not clear to you, if there are things that you would like me to explain a little bit further, if you have any just general questions, please take advantage of that Q&A box.

My goal for today is we want to make sure that each of you come away really feeling like you understand the way that this applies to your practice. If you have a specific

File name: HIPAA Compliance Lessons and Breaches in 2022.mp4

need, we want to make sure that we tackle that as well. We're not always able to get to every question, but just want to make sure that this is as relevant for you as possible.

First thing we're going to talk about: general HIPAA compliance. As a small practice, the majority of you, let's say, being either solo small practices or maybe a handful of staff, what do you actually need to be doing for HIPAA compliance? One of the biggest difficulties, when you're talking about HIPAA compliance for very small practices, is that you're dealing with a regulation that could apply to the largest regional hospital group or insurance company in the nation, but could also apply to you as what might be a small solo practitioner, and then every other type of entity in between.

The expectation of HIPAA and the government, the way that they designed it, is it's really been published as very broad, intentionally vague guidelines because to the government, this is not just about checking a bunch of things off of a box and saying that you did it, it's a matter of practically understanding those requirements and implementing them into your practice in a way that will be effective for you, and that's even why this document that you see here on the screen, what do you need in order to be HIPAA-compliant?

You need an effective compliance program, and even that term "effective compliance program" means that what's effective for you is going to be different than what's effective, let's say, for a really large hospital group, but where a lot of people go sideways is they interpret that as meaning that they can do less than what the law requires, and that's not the case. Everybody has to address the same requirements, everybody has to follow the same guidelines, it's just the way that you implement it in your situation is going to be somewhat unique.

If we take all of these different elements and break it down into a very simple framework you can follow, basically, what HIPAA compliance requires, first and foremost, very foundationally is that you are documenting an annual risk assessment. That can sound intimidating, but basically, this is just the government's expectation that once per year, you are expected to document a review of things like your policies, your procedures, your trainings, review your devices and your IT, make sure that everything is secure, and I say, make sure that's clearly documented because to the government, that's really why they require this.

Their expectation is not just that you're doing these things in practice, but that you want to be able to prove your compliance on paper. Doing that annual self-audit and review and documenting that process, documenting where your gaps were, how you are addressing them, that is really what builds the basis for what the government calls good faith effort. That's basically your ability to show proof that corresponding to what the law requires, you have made a good faith effort to address those requirements.

There's another huge benefit there which is, doing that assessment allows you to know and prioritize where you actually might have issues in every other area of your compliance program. You might be coming to this, you don't even know what policies and procedures you need to have for HIPAA. By going through that assessment,

you'll identify what the government expects and what you need, what trainings you might need to have for yourself, maybe trainings for your staff.

HIPAA has very specific requirements around your vendors, business associate agreements, how you handle incidents, and it's a very multi-layered thing. One of the best ways that you can simplify this within your practice right now is just doing that risk assessment once per year. Technically, the term that the government uses for this, it has to be an ongoing assessment. Really industry best practice is do an audit once a year, make sure it's clearly documented, and then just keep it up to date throughout the year as you move along.

That is the simplest, fastest, and most effective way to create an effective compliance program within your practice, especially for small practices. Even if you want to take a screenshot of this, we as well have a very simple HIPAA compliance checklist that's like a one-page overview of all of these requirements. Following that workflow really puts you in a position where you can just have peace of mind that you're checking all of these boxes.

Now, to talk about where some of these things go wrong as far as HIPAA compliance is concerned, I'll say, we are really only going to just skim the surface of some of the more prominent published finds. Of course, not every government settlement is public record, not all of this is published, we're just going to look at some of the bigger ones that were put out this year. We can have some key lessons and takeaways that you can bring back and apply.

Now, in terms of-- and I know probably a lot of you are even wondering, how do you even get audited? What causes a HIPAA audit or investigation? Health and Human Services is the government entity that writes the regulations. The OCR is the enforcement body of Health and Human Services down to the state level, which would be the state attorney generals. If any of you are billing Medicare or Medicaid, the CMS can also do HIPAA and compliance-related investigations as well.

There are a few different ways that you can get on the radar for, let's say, a HIPAA audit. One of them could be your vendors, meaning it might not be an issue within your practice, it might have been one of your business associates or a vendor that you're using had a breach, it compromised your patient's information and you didn't have business associate agreements in place, that gets a lot of people in trouble. Could also be just a random audit. The government does do random HIPAA audits and investigations that is usually extremely rare-- for anybody that is on this webinar, if you are more of a small practice, it would be so rare for you to ever be randomly audited.

It's usually something that has to take place to kick it off, meaning a breach, could be an issue with a CMS if you're getting Medicare. The number one way that we see practitioners though being audited for a HIPAA issue is in the event of a patient complaint. This is particularly common in the behavioral health space because you are dealing with extremely sensitive information. Those types of scenarios can sometimes go volatile very quickly.

A patient files a complaint against you, and the OCR is required to investigate all of those complaints. Usually, what they'll ask you for, first and foremost, is a copy of your annual risk assessment documentation. That's why we always say to begin there. Now, this past year in particular, there was a particular enforcement initiative of the government that really changed the landscape as far as HIPAA enforcement is concerned.

We'll start by talking about how, let's say, two particular case studies in the behavioral health space, solo practices where this occurred, and then we'll broaden it out and look at some other general case studies of what's taking place and some key takeaways. There was something that was started three years ago by the OCR called the Right of Access Initiative. The Right of Access Initiative, if you're at all familiar, is very closely tied to something called the 21st Century Cures Act, which basically has two things.

It's trying to promote what's called interoperability, meaning that it should be easy for patients to be able to get access to their healthcare records. Then number two, it specifically prohibits a practice known as information blocking, meaning a practice cannot put anything in place that inhibits or prevents a patient from being able to get access to their own medical records.

You see two particular cases here. Again, these are just two of the ones that were published where a company by the name of Jacob & Associates, medical records were withheld.

A patient was requesting their information and they were actually being told that they needed to pay money to get access to those records. In this particular case, not only were they withholding that information, it took them a very long time even after charging the patient for those records, and the patient filed a complaint. In the end, it was found that this particular practice was not following those Right of Access requirements. They did not have policies in place regarding Right of Access and the privacy requirements for HIPAA.

It led to a pretty hefty fine, it was a \$28,000 fine. Now, an interesting thing in this flip side, Danbury Psychiatric Consultants was fined \$3,500 because they were withholding medical records because a patient hadn't paid their bill. In the end, the only reason why the fine was as small as it was-- this particular fine is the smallest fine actually in the history of HIPAA compliance, never been a fine as small as this one. Usually, you're looking at-- 28,000 is an average if you're a small practice, all the way up to much larger depending on how cooperative you are.

In the case of Danbury Psychiatric Consultants, the only reason the fine was so small was because they were extremely cooperative with the OCR's investigation process. They were very lenient in this case, \$3,500 fine. We're going to look at some additional here, and then we're going to really dig into key takeaways and the ways that you could apply this.

There were other scenarios. A dental practice, which was using a third-party marketing company to essentially market their practice, they shared all of their patient's information with this marketing company. The marketing company was

actually using that patient information to run ads through Facebook. In the end, they were-- again, there was a patient complaint. The government started digging into all of those processes and figured out what was going wrong.

They were fined \$62,000 because number one, they were utilizing a marketing company that was essentially marketing to their patients in a way that was totally not HIPAA-compliant. We'll talk about this a little bit later on. Need to be very careful, especially from a marketing perspective, how you use your patient's information, and that if there is anywhere that your patient information is being sent to or stored, that you have a business associate agreement, you make sure it's being protected. In this case, a lot of those things were missing. They also had not done a risk assessment, did not have HIPAA policies. \$62,000 fine.

In the case of Dr. Phillip, I'm not even going to try to pronounce that last name, but another small practice that had replied to a Yelp review. There's been several instances of this that have happened. Let's say that as a practice, you have an online presence, and one of your patients has a negative experience with you, and they go online and they leave a negative Google review, or they leave a negative Yelp review. Something like that.

According to HIPAA regulations, your patients can do whatever they want. They can go online, they can put their own information out there. Where you need to be extremely careful is in how you are replying to those types of reviews. In this case, this particular doctor replied to this negative Yelp review and confirmed information about the patient, further expounded upon the particular situation in an attempt to defend himself. The patient actually reported him because he disclosed what was really private information in an online forum, in an online review. \$50,000 fine.

The general takeaway here is if you have any type of a social media presence, Facebook, Google, Yelp, whatever it is, you want to be really careful in, number one, making sure that you're not openly plugging in patient information into those platforms like this marketing company did, but also be very careful how you respond to your patients in those online forums. Your patients can really disclose whatever they want on Facebook or on Google or on Yelp, but you will be held responsible for your replies.

The general rule of thumb is to keep your replies completely anonymous. Do not even use the patient's name. If John leaves a review that says that he had a horrible experience, simply reply and say, "Sorry, we apologize for your negative experience at the practice. Please contact our office, so we can discuss." Don't get into the scenario, don't dig deeper. You want to keep it anonymous, very simple, to the point. "Please contact our office."

Same even goes with positive reviews, like just even replying, saying, "Thank you for the kind feedback." Don't give a bunch of information, don't use the patient's name. Make it very simple, very straightforward. Two more. These ones, I think, give some good insight as far as broader HIPAA implications. New England Dermatology and Laser Center was incorrectly discarding containers, labels, and patients' PHI. In this case, it was actually particular labels and paper records that were being discarded

through non-HIPAA-compliant means. Basically, they were just throwing it in the garbage.

What happened is somebody came across legitimately the trash and found all of this sensitive data in the trash, reported the company, and they were fined for missing policies and procedures. Most of you, in this case, you should have a shredder, make sure at a bare minimum that any paper records you're disposing of were actually being shredded, but an interesting takeaway in most of these cases is that this practice was not fined because they made a mistake.

They were fined because, in their audit, they were found to not have implemented the required policies and procedures that they need for a HIPAA compliance program. In this case, it was a larger, well-established practice. This impacted legitimately thousands of patients, so it was a very hefty fine. Something to be on the lookout for.

Lastly, Oklahoma State University has a medical branch where there are residents and providers seeing patients, and there was a complaint filed against them due to a breach that had occurred and affected legitimately thousands of patients. In the government's audit, it wasn't just the fact that they had a breach. Again, it was the fact-- and this scenario was kind of a mess, it's the fact that they had not done their annual risk assessment. They had not documented how they were remediating issues found in that risk assessment. They did not report the breach in a timely manner. They didn't have the right safeguards in place.

A lot of things going wrong here. Another pretty hefty fine, but the key takeaway is in a lot of these cases, none of this had to happen if they were doing an annual risk assessment because even the case of the Right of Access stuff, if you're doing an annual risk assessment for HIPAA and auditing your own policies, figuring out what you have and what you're missing, you'll be in a position where you actually know that, "Hey, we should implement a Right of Access policy," make sure that we have a documented process for this, that we're keeping among these requests.

We're going to continue to go deep into some of these lessons, but that's to start. Now, what caused a majority of the breaches in 2022? We're going to cycle off of some of the fines and talk about breaches in and out of itself because there are some important implications here. Then we're going to start going deep on actual lessons and takeaways.

What caused the majority of the breaches in 2022? The majority of it was hacking and IT incidents; reported more than any other breach. October in particular was a terrible month. 6 million records breached, and that's only what we know based on what's published publicly. An interesting thing that's important to keep in mind though is that a lot of people-- "Hacking in general and IT-related issues continues to be the greatest threat." This is a quote from the OCR's director, Roger Severino.

A lot of people think in the event that there's a cyber predator, you see the movies, people hacking in systems, and all of these things that are taking place. When we talk about hacking, particularly within healthcare contexts, there is almost always a human error component to it, that is what actually allows a hacker to gain access into

your system. Email phishing is the biggest cause of this, meaning you get an email in your inbox, it looks like it's from a company that you're contracted with.

It has you click on a link and then turns out that link was a very suspicious provider, and by clicking it, you just gave somebody access to your system. Something very common that happens is called a ransomware. In a ransomware attack, they actually would crypt your entire system, all of your data, and make you pay a ransom before you're able to get access back into your own systems.

That human error side of things is another thing that you really can adequately address through a HIPAA compliance program. Part of what HIPAA requires is security policies as well as general cybersecurity training. If you're not doing, let's say, that cybersecurity training, you might not even know how to recognize a phishing attack, how to prevent a ransomware attack.

An interesting statistic, 94% of all practices that had a ransomware attack had antivirus and anti-malware software installed. Only 10% had actually done a cyber safety training. That's another thing really worth looking into for you and your staff. If you're looking to prevent some of these breaches from happening, the most important thing that you could do is address that human error component, make sure that you're doing a cyber safety training with your staff. That'll be really beneficial in educating them, just to make sure you don't have these issues.

A lot of this comes down even to a general misunderstanding in the dynamic between compliance and security because security is-- you could think of it as your technology. It's risk mitigation, making sure that from an IT perspective, that you have everything that you need, and that in a sense controls your risk. Compliance though is very different from security in the sense that it's binary. It is really more about your ability to show clear documentation, that you have satisfied the requirements of the law, that you've implemented policies, that you have training records for you, and for any staff that you might have.

Along these lines, those two things brought together compliance and security, so it really puts you in a position of safety and peace of mind. It's good to look into both sides of this. HIPAA Right of Access fines is the number one way that practices got fined in the last year, particularly small practices. To talk about-- as we get into some key takeaways here, how do you protect yourself from a Right of Access fine if a patient's requesting their information?

Number one is just even from an ethical perspective, we have to respect an individual's right to access and receive their own medical records. There are some exclusions specifically in the behavioral health space around psychotherapy and therapy notes, meaning your patients don't have the right to access your personal therapy notes about your interactions with them. Hopefully, that gives you all a lot of peace of mind, but there are general records, invoicing, treatment records, things like that, we need to respect the fact that patients have the right to access that information.

Second thing is in the event that you receive-- a patient requests for information, you have to reply and provide those records within a timely manner. The general

framework that the government expects for this is that it's within 30 days. If you're not able to do that, seek an extension. When we say seek an extension, what that really is, is just notifying the patient that it may take you some time, request an extra 15 days, and make sure that you have documented that you sent through that request.

Third, make it easy for your patients to request those records from you. Even if you set up an online patient portal, or if you just create a process where they email you, and either yourself or somebody in your staff can reply and send that through electronically, that makes it a lot easier. There are specific allowances where you can charge patients for those records. That varies state by state though, so I'm not going to give specific guidance on that. If you want to learn more about that, you can speak to maybe a lawyer locally about the different state guidelines. In general, you're not going to make a lot of money off of sending a patient their information. It's also not a bad thing to just do it for free.

Now we're going to get into some key lessons. I'm going to try to make this as specific as possible for psychology practitioners, for those of you that are on here with very small practices, trying to figure out how to navigate some of this. First thing is that really all providers right now are at risk of being investigated for a HIPAA violation. Four years ago, that was not the case. Four years ago, probably 95% of all of the HIPAA fines were to the larger healthcare groups, and that has completely changed now. More than 65% of all of the OCR settlements in 2022 were with either very small or solo practices, so 25 employees or less.

The Right of Access initiative really changed that dynamic. Also, in general, small practices tend to have more vulnerabilities because your patient information is still just as valuable to a cyber predator, but you might not have all of the infrastructure of a larger group to protect it. It's really good to start taking this seriously now, particularly again, if you don't know how you're going to complete your HIPAA risk assessment this year, start looking into that because that's the best way that you could just protect yourself from a HIPAA audit in the event of a breach to have really solid documentation.

Number two, in general, not cooperating with an HHS or OCR investigation will cause your fines to be larger. Among very small practices that cooperated, again, we saw maybe \$3,500, small practice ACPM Podiatry was issued a \$100,000 fine because they received two complaints and didn't even respond to any of the OCR investigation requests, and they reached out to them many, many times. You can damage control by just making sure that you're very responsive. The government is usually lenient with people that are reporting their issues, responding to their auditor, and makes it really simple.

Number three, keep a log that actually tracks access requests and how you are responding to them. That automatically shows Health and Human Services that you are taking your Right of Access obligations seriously. If a patient requests their records, and they're looking to see your notes, remember that you do have an exemption around your specific therapy notes that you take in your sessions with your clientele, that's important.

Number four, a patient may only be charged a reasonable cost-based fee, that's a term that the government uses, when requesting their own records for their own use. What does this mean? It means that if your patient is trying to actually see another practice for services, and they want to make sure that that practice has access to their previous history with you, you cannot charge them for that. The government does not allow it. It's only if they're asking for that information for their own personal use that you could charge that type of a fee, and again, that varies state by state.

Lastly, all providers need an effective compliance program. Small practices, large groups, everybody in between, the regulation of what it requires does not change. What will change is what's effective for you and what this winds up looking like practically, but you still need to have very clear documentation of good faith effort in the event that an audit happens. That's the only way you can prevent a fine. The government does not care, again, what you're doing in practice. What matters is what you can prove on paper.

The easiest way to start that process, if you don't know where to begin, is by completing that annual risk analysis or risk assessment and addressing the gaps that were found, and clearly documenting those efforts. In general, some predictions, there's a couple of things that we see happening in 2023. Number one, the government is really still going strong on the Right of Access stuff. There's already been a bunch of fines this year. There's a lot being published and a lot being talked about. I think that we're going to continue riding that Right of Access wave for a long time.

To highlight a couple of things that is just interesting, you see a huge uptick in this Right of Access initiative. From 2019 to 2020, there was a 450% increase in Right of Access fines. Even in the middle of the pandemic, up to that point in time, 2020 saw more HIPAA fines levied than any other year in the history of HIPAA compliance. 2021 then beat that record. 2022 beat 2021's record. This is not slowing down.

One of the main things to be thinking about, make sure that you have all of the privacy policies that you need for HIPAA that include Right of Access, that you keep a log of all of those requests, and that you respond appropriately because the government's going to continue looking at this. As well as the Dobbs decision. I'm not going to go too deep on this, but the Dobbs decision has some very broad implications for the healthcare space.

Specifically, let's say, in the event that you have a patient complaint, and you could even just read this here, it's going to be putting more emphasis on responding to patient complaints that allege that providers have improperly used a patient's PHI without authorization. Basically, meaning that very, very broadly if your patients are requesting records for all sorts of different things, the implications of the Dobbs decision, very closely tied to Right of Access, is that you have to provide that information.

Specifically, what this means is that you have to provide that information to any government entity that is requesting it. In the event of some type of complaint through an investigation, the Dobbs Decision means that whether it's OCR, CMS,

state attorney general, local government, government authorities, if that's what's happening, you have to provide that information and cooperate.

Lastly, we're going to wrap this up here, talking about that social media marketing topic, I think that there is a huge benefit for all of you in marketing your practices, but you have to just make sure that it's being done properly. Particularly, the Facebook Pixel was found to have literally tens of-- and the Facebook Pixel is Facebook's online marketing solution and their tracking tool. Tens of thousands of patient records were found on Facebook Pixel, it was a big deal, lot of practices, lot of marketing companies, Facebook themselves got in big trouble.

Going forward, if you decide to market your practice, it's a good idea to just make sure that any marketing that you do is completely anonymized, that it is not specifically targeting specific people. If you are going to be taking a more in-depth or proactive marketing approach, it's worth actually just using a marketing company that has HIPAA expertise and is willing to sign a business associate agreement with you. That's going to be super important.

With all that said, hopefully, I know that probably it's not the highlight of your day, sitting in on a 45-minute presentation on HIPAA compliance, but what we're going to be doing now is-- hopefully, it wasn't that dry and kept your attention. What we're going to be doing now is actually just taking some questions. Robin, I see a lot of questions coming in, so if you'd like, we could start tackling those now.

APA/Robin Tiberio: Absolutely. Thank you so much for your presentation and we'll get jumping in on some of these questions.

Liam Degnan: Awesome.

APA/Robin Tiberio: To start with, could you provide some more specific guidance on use of email and text messages when communicating with clients?

Liam Degnan: Okay. Email is a tough one. There's a few very general broad stipulations and guidelines. My assumption is that the majority of you on this webinar are either using Gmail, email, or Outlook through Microsoft. The primary rule of thumb when it comes to email is if it's free, it's not HIPAA-compliant. If you are using a free Gmail or a free Outlook account, and you are actually interacting with patients in that format, that is not HIPAA-compliant and can get you in trouble.

Simply by upgrading to the paid business version of Gmail, in this case, I believe it's Google Workspace, and Google will sign a business associate agreement with you. The other thing you would want to make sure is if you're-- particularly, if you're exchanging sensitive information, you would want to have some sort of email encryption service installed on your email. These are super cheap most of the time.

There's several companies that do it. It's probably a couple of bucks a month, plus the Google upgrade, and then you have a fully HIPAA-compliant email. Text messaging is the same thing. There really isn't a context in which SMS is compliant unless you are using a third-party vendor that is specifically providing HIPAA compliance text messaging services and is signing a business associate agreement

with you. Even for things like patient scheduling and things of that nature, that's a really important dynamic to take a peek at.

Now, just make sure that you have the right BAAs and that all of that is set up. Real quick, Robin, I'm seeing some questions coming in just clarifying, looking for clarification on some of the email guidance, I can maybe just tackle one of these quickly. I saw it come in and I thought it might be helpful for everybody.

APA/Robin Tiberio: Yes, absolutely. The one on Gmail?

Liam Degnan: There was a question that came in that with regard to emailing people. Is every email sent subject to HIPAA? For example, is sending an email about scheduling subject to HIPAA regulations? The answer to that question is yes. HIPAA has passed very specifically to protect PHI.

What's PHI? PHI as far as the government is concerned is that if you are a covered entity, meaning, in this case, if you're billing insurance for the patients that you're seeing, all of your patient's information is protected. Even their name, their phone number, their email, it's all considered PHI. Even in that context, if you're not specifically sharing a ton of sensitive information or just are scheduling an appointment, still something that really needs to be set up in a way that's HIPAA-compliant, so just wanted to clarify that quickly.

APA/Robin Tiberio: Thank you. All right. Also, getting some questions on-- What advice would you give to a professional starting their own practice, and particularly smaller practices, about the best strategies for managing HIPAA issues?

Liam Degnan: The general best strategy, and let's say number one, if you're a startup practice and you're just getting off the ground, but also for any of you that are on here that, let's say, are just starting from scratch for HIPAA, a great place to begin is going to be that risk assessment. There's lots of different methodologies for doing that. There is actually a free resource through the government that just gives you an outline to follow as far as what you need to be checking for your risk assessment, and that's something that our company can help with as well if you were looking for an easy way to do that.

APA/Robin Tiberio: Awesome. Thank you. Could you describe the process of an audit? How does the OCR select, approach, and manage an audit, and what support is out there for someone being audited?

Liam Degnan: The general process of an audit, it's two things. Initially, you get on the OCR's radar like we discussed, a patient complaint, a breach happens, a vendor issue, things like that. Usually, the first thing that occurs is the government will conduct what's called a desk audit. In the event of a desk audit, they're going to ask you for some basic documentation.

Usually, what this is, is a copy of your risk assessment records from the last couple of years. The reason why that risk assessment is so important is because you can stop the audit right then and there. If you have adequate risk assessment records and you are able to send those through, the government probably will not even

investigate you further. It's only if they find issues in that initial desk audit that they will then have a follow-up and go much, much deeper into all of the other stuff in your practice. That could be vendors, policies, processes, the whole thing. That's what you want to be thinking about.

APA/Robin Tiberio: Seeing a lot of questions coming through about how you can determine if an audit is legitimate or not, and it's coming from a legitimate place or if it's a scam?

Liam Degan: That's a really good question. Unfortunately, again, there's a lot of predators out there. One of the things that you want to keep in mind is you will never ever be notified of a HIPAA audit via phone or via email. You will receive a letter in the mail, specifically from the OCR. You would just want to verify the mailing address. If you see that type of a letter come in the mail and it's all verified, it's from the OCR, the same address, it all lines up. You're going to want to reply quickly.

APA/Robin Tiberio: What is one important but often overlooked way that small practice owners can reduce their liability or likelihood of a breach?

Liam Degan: A simple but often overlooked way. I think in general, what happens sometimes in small practices is you might have HIPAA policies in place, but the policies maybe came from another practice. They might have been just a store-bought HIPAA manual. It may not have been updated in a bunch of years. Simplest thing that you could do is just make sure that if you have HIPAA policies, that it's not just like a paper manual, you want to be able to actually manipulate them in a Word document format so that each year, you can do an update to those policies and that you log that that update took place. That alone shows a ton of good faith effort just by making sure that you're just not using the same paper policies every year or a manual that's not being updated or reviewed.

APA/Robin Tiberio: Also, getting-- I've seen this a couple of different times in the Q&A box. The intersection of HIPAA and doing forensic work with the courts. How do those two things work together or intersect?

Liam Degan: It depends on what your contract looks like with the court. Oftentimes, forensics-type work is not necessarily covered under the umbrella of HIPAA because specifically what makes you a covered entity for HIPAA is if you are processing a covered transaction. In this case, a covered transaction meaning your billing insurance, and those transactions are going through an insurance company.

If that's not taking place, still if you're doing forensic work on behalf of the court, let's say that they're asking you to sign a business associate agreement or they are requesting that you be HIPAA-compliant as part of the contract and confidentiality, that's the primary intersecting point because if you're signing a business associate agreement with those entities, then you're legally obligated to make sure that you have all of these HIPAA compliance requirements set up. I'll be transparent, I'm not too familiar with the forensic side of things. I've worked with several practitioners that were involved on both sides of it, so I've got a little familiarity. That to me is the bulk of what I've seen.

APA/Robin Tiberio: Thank you so much for all of your great questions, getting so many. Another question I've seen come through quite a bit is about social media reviews, online reviews, and how you deal with that. Aren't you confirming that they're a patient if you respond to an online review, and how does that work?

Liam Degnan: Just looking for general guidance a little bit deeper on the social media stuff?

APA/Robin Tiberio: Yes, that's what it sounds like.

Liam Degnan: The best way to think of it is keep any and all of your replies to patients online fully anonymous. Don't use their name. Don't even say, "Thank you for coming into the practice today," things like that because then you're confirming that they came into the practice. All of that stuff, you want to keep it very simple, to the point. If it's negative just say, "Please contact our office, so we can discuss this." In an online forum, again, there's been a bunch of HIPAA fines that were published due to the online review issues, you just want to be really careful and basically anonymize everything.

APA/Robin Tiberio: Thank you. Also getting a lot of questions about how much do someone need to do or worry about this if they don't take any insurance, if all clients are self-pay?

Liam Degnan: Good news is that if you are an exclusively private pay practice, you are not covered under HIPAA. There's two sides to that. You are not legally obligated to address the full extent of these requirements. Certainly, you still want to have a minimum expectation of privacy and security because you're still dealing with sensitive information, but specifically, it is billing insurance and processing those transactions that makes you a covered entity under HIPAA.

HIPAA itself, and a lot of people go sideways on this, HIPAA itself stands for Health Insurance Portability and Accountability Act. Originally, it was passed to only provide to the insurance companies. The definition of a covered entity was then broadened out to include any providers that were billing insurance and then even further broadened out to include business associates or vendors.

That's some good news, but just in general, a lot of practices often start private pay. It's not a bad idea to just set these things up off the bat because if you ever want to become insurance approved or you see yourself growing into that type of a business model, having these things set up ahead of time just puts you in a position where you know even in the event of a liability situation with a patient, you have really rock solid documentation, and then you're set up and in a position where you could easily transition to accepting insurance if you wanted to.

APA/Robin Tiberio: Great. What else? Also seeing a lot of questions about dealing with patients who probably have been advised that they should not be communicating via certain methods but still insist on doing so. Is there any potential liability there?

Liam Degnan: The only liability that you have is if your setup is not compliant. If a patient decides to email you, that's on them, but let's say your email service should still be HIPAA-compliant or you should be leading those emails and blocking them from emailing you, blacklist them, and the same thing goes for text messaging and things like that. You are really only responsible for what you are doing. If a patient opts to continue pursuing you via text message or via email, you can only really get in trouble if you're replying to them, and the setup that you have for that is not HIPAA-compliant. Hope that makes sense.

APA/Robin Tiberio: All right. Also getting a lot of questions asking for some additional clarity around what client records are okay to withhold and what needs to be available should they be requested.

Liam Degnan: This is one of those vagueries within the regulation. It's very broad, the definition of psychotherapy notes or therapy notes. I would recommend if that is a particular concern of you, I would actually speak with your lawyer because some of this can get a little fuzzy depending on how it's set up within your practice as far as what is considered therapy notes and what is not. I'm not in a position to dig into all of the nuances of that on this particular webinar today, but of course, if you need particular help on that, please feel free to contact the lawyer. You could reach out to me directly as well.

APA/Robin Tiberio: I've also gotten a question about, could you further discuss the Cures Act and how that intersects with HIPAA?

Liam Degnan: Under HIPAA, you have the privacy rule. The Right of Access initiative is an enforcement initiative enforcing aspects of the privacy rule related to a patient's right to access their information. The 21st Century Cures Act is not under the umbrella of HIPAA, but it is still a Health and Human Services regulation that is enforcing those same privacy rule standards, but it adds some additional layers to it in the sense that it not only prohibits either a provider or an EHR from information blocking or preventing information being accessed by a patient, it's promoting something called interoperability, meaning it should be easy for patients to get access to their information.

This also is closely tied with Medicare incentives for switching to the cloud and EHR-based things. They're kind of communicating the same thing. It's just a separate regulation to add additional layers of focus on the side of Health and Human Services.

APA/Robin Tiberio: All right. We're getting in the last couple of minutes here, so I'm going to combine this all into one question. We've gotten many, many requests for templates or guidance on a list, your annual risk assessment resources for good cybersecurity training, and then also if they have further questions or need further guidance, contact information for you, Liam. I'm going to roll that all into one question. [chuckles]

Liam Degnan: Like mentioned at the beginning, I'm with Compliancy Group. We are the APA's preferred provider for HIPAA compliance solutions. We work almost exclusively with small practices, so small midsize practices is our focus. Our program

is like the idea of having TurboTax or QuickBooks, but for compliance. Specifically, if you're looking for a nice easy way to do your risk assessment, automatically setting up your policies, training, BAAs, our solution, we have a very automated process. We provide you with a dedicated rep on our end. They walk you through everything.

It's designed to be as affordable as we can make it. We do have a landing page with the APA. I don't know if we have the ability to send that into the chat. If you'd like more information on that, you can just go on our website and request some information, compliancegroup.com. You can, of course, as well, email me directly. My email is just liam@compliancegroup.com.

APA/Robin Tiberio: Great. If you had joined us earlier in the chat, if you scroll down, under the Additional Resources header, we have those two links that Liam just mentioned there, that HIPAA checklist, and then also a request for more information if that is of interest to you. Let me just see if anything else came through. Looks like a couple of questions about if superbills make any difference to HIPAA and insurance and private pay. That's come through.

Liam Degnan: I'm assuming that maybe that's referring-- I'm not familiar with the very specific terminology, but if you're referring to, let's say, you provide services to a patient and you provide them with a bill, and then they seek reimbursement for that bill through their own insurance providers, still that it does not come back to you, that's the patient themselves taking that, trying to process it through their own insurance company. If you're private pay, this is not going to be a huge concern for you, unless you intend on billing insurance in the future. Then I would recommend actually setting it up now ahead of time. If you're billing insurance, those of you on here, that's who should really be concerned about this.

APA/Robin Tiberio: Great. Would you mind repeating your email one more time?

Liam Degnan: Yes. My email is legitimately just my first name at compliancegroup.com.

APA/Robin Tiberio: liam@compliancegroup.com for everyone on the line. Thank you. All right. Well, thank you so much, Liam. We really appreciate it. Thank you so much for all this great information and for answering all these questions. Thank you to everyone on the line for submitting your great questions. We really appreciate all of the interactions. Thank you to--

Liam Degnan: Thank you for having me.

APA/Robin Tiberio: Oh, sorry. Go ahead.

Liam Degnan: No, thank you for having me. This was great.

APA/Robin Tiberio: Thank you to Compliance Group for making this webinar possible today. As we've mentioned before, a recording of this presentation will be emailed to everyone in about two weeks' time. That recording also includes a copy of the presentations live. As soon as the webinar has ended, a short survey will appear on your screen. We ask that you please take the survey and give us your feedback.

With that, we thank you so much for your attention and we hope that you have a wonderful rest of your day.