

HIPAA Compliance Pays Off: Why You Should Invest in Compliance

Date & Time: Dec 5, 2023 01:00 PM Eastern Time (US and Canada)

APA: Hello, everyone, and welcome to today's webinar, *HIPAA Compliance Pays Off: Why You Should Invest in Compliance*. This webinar is paid for by Compliancy Group, APA's preferred provider for HIPAA compliance solutions. Compliancy Group gives psychologists confidence in their compliance plan, which increases patient loyalty and business profitability while reducing risk.

Some important points before we get started. Liam Degnan, the presenter for today's webinar, is a senior sales engineer at Compliancy Group. As such, he has both a financial and intellectual interest in the content. The purpose of this presentation is to provide a balanced view on HIPAA compliance. APA does not endorse any products or services. The content was created by Compliancy Group and does not reflect the views of APA nor its editorial staff. Please email advertising@apa.org if you would like to learn more.

Next, 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. A recording of today's presentation will be emailed to everyone in the next two weeks. The email will also include a copy of the presentation slide.

In 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. We will put a link to the presentation slides in the chat box on your webinar screen. If you miss them, we will email them to you along with the recording in the next two weeks.

With that, I would like to introduce today's presenter, Liam Degnan. Liam has eight years of experience combining risk management, SaaS sales, and regulatory compliance in the healthcare space. As Compliancy Group's Senior Sales Engineer, he advises healthcare decision-makers, healthcare providers, and medical vendors. He speaks on a variety of platforms and topics with an emphasis on simplifying HIPAA, OSHA, SOC 2, and other general healthcare compliance regulations. Welcome, Liam.

Liam Degnan: Thank you so much for having me. I'm happy to be here, folks. As mentioned, really, the topic that we're going to be going over today is really dealing with the ways that taking compliance seriously can benefit your practices. One of the things that I would like to say just to start is first sincerely thanking the APA for having us here. Also, I, just in general, at Compliancy Group, we work with a lot of different types of healthcare specialties. We as well have engaged with many different associations and wanted to just sincerely say at the opening here that the APA is among the best of the best.

The level of care that they have and their desire sincerely to bring the most value as possible to their members is something that you really don't see that often within healthcare associations. It almost borderline does not exist. You should all be very

proud of the profession that you're in, but also of the association that you're a member of because the APA is fantastic. We are really, really happy to be here.

Like I mentioned, to give a quick synopsis here what we're going to be going over, to give you a general landscape as far as the topics we're going to be covering today and what you can expect. We're going to begin here by giving a general lay of the land as far as introduction to HIPAA compliance and some compliance basics, just to set a really clear baseline foundation for the rest of our conversation for today.

We're going to talk particularly then transition into some common pitfalls depending on the size of your practice. Probably the overwhelming majority of you on here are either solo practitioners or maybe you have just one or two or a handful of employees. Some of you might be slightly larger than that. We're going to talk through some of those different scenarios and what the most common things we see being missing within those different environments.

From there, we're going to look at some real-world case studies as far as behavioral and mental health practices that were audited, that were fined for compliance-related issues, and what some of the key takeaways there for you are, common violations, and then benefits as well as risks. Our goal for today, and I mean this, is to be as practical as possible. My goal truly is that you come away from this webinar with actionable to-dos within your practice, that you have a clearer understanding of what you might be missing, to give you some peace of mind, right?

That's really the goal here with all of compliance is we're not trying to scare anybody into complying. We want to give you actionable next steps that you could follow to protect your practice and give you that peace of mind that you might want or need, right? Not just for you, but also really for your patients. That's one of the things that we'll talk about as we go through as well is one of the things that's really irreplaceable, especially if you are a very, very small practice, is having a genuine desire and a genuine care for your patients and a desire to make sure that you are protecting their information, that you're taking these things seriously and we'll go through there, okay?

I'm just seeing a couple of chats here. Okay, just making sure that was handled. All right, so without further ado, we'll go ahead and jump into the content. Please, please take advantage of the Q&A box here. If there's anything that I talk about throughout the course of this presentation that is either not clear or that you would like us to circle back on and give some more information on, I am more than happy to do that.

When we finish this up at the end, the end of the webinar, we'll have plenty of time for Q&A. We also received some questions ahead of time that I'll tackle before we dive into the live questions. Seriously, if there are things that you're hoping to get out of the webinar today, go ahead and send those things into the chat because we would really love to tackle it with you just as we go through or at the end.

Now, without further ado, introduction to HIPAA compliance. All of healthcare compliance is regulated primarily by two entities. That is the Office of Inspector General as well as Health and Human Services. All of that rolls up to the Department

File name: GMT20231205-180008_Recording.cutfile.20231206140650565_1920x1080.mp4

of Justice and then there's an enforcement branch for HIPAA that is known as the OCR, but really the one who actually makes and develops these regulations is Health and Human Services and the Office of Inspector General. What they published as the highest-level boilerplate requirement of a compliance program is something that's commonly known as the Seven Fundamental Elements of an Effective Compliance Program. That's what you'll see here on the screen.

Now, one of the things I'll highlight before we even get into the ins and outs here as far as these individual elements in and of themselves, one of the really, really important things to point out is actually just this word effective. Particularly for those of you that are very small or solo practices, one of the things that makes HIPAA compliance uniquely challenging is that the regulations don't change. You are dealing with the same regulations that could apply to you as could apply to a large regional hospital group or a health plan and everybody else in between.

The regulations in many ways, because of how broad they are, were really written in a way that is almost intentionally vague because they have to apply to a very broad audience. In that sense, the process of becoming compliant with any regulation, but let's say HIPAA specifically, as published by Health and Human Services, is not simply just checking things off of a box for the sake of saying that you did it, but really a function of understanding what can sometimes be, yes, broad, vague guidelines and implementing them into your practice environment in a way that is effective for you.

Because what makes sense for you is not going to make sense for somebody else, right? If you're doing what a large hospital system is doing, it would obviously be a whole ton of overkill. Even just you compared to a practice up the street with a different environment and different methods of treatment, let's say you have an environment that's more oriented around telehealth as compared to in-person visits, your needs and how you ultimately set up your compliance program will be different, but the general framework is the same, right?

First is the implementation of written policies, procedures, and standards of conduct. In essence, what are you complying with? You're complying with your policies and procedures, right? Your internal policies within your practice, this is one of the first steps in setting up a compliance program, is making sure that you have policies that are a clear reflection of the law, but also a clear reflection of your operations.

It's very common for practices to purchase, let's say canned policies that are not really manipulated to be an accurate representation of their environment. That's something that you want to stray away from. It's okay to purchase policies and then manipulate them, right? If you're truly just using like a store-bought manual and it's just sitting on a shelf somewhere, that can be problematic because it's not effective, right? It's not actually a clear representation of how you operate.

Now, all of these other things, so designating a person to ensure they are followed, if you're a solo practice, obviously that's probably just going to be you, right? Conduct effective training and education and lines of communication, again, those are going to apply to those of you that have staff. This could be one employee or many, doesn't really matter what it is.

Number five is often like the linchpin of the program, which is conducting internal monitoring and auditing. We'll talk a little bit more about what that means from a HIPAA perspective as we go through, but in essence, HIPAA requires that at least once a year, you're doing some sort of internal audit or assessment for your practice, especially for those of you that accept Medicare. This is something that is also a requirement under MIPS if you're enrolled in MIPS. That annual assessment is how you actually prove what you're doing each year, something called good faith effort in the eyes of the law so that you could show that you're making progress each year, that you are practically addressing these requirements.

Then these last two deal with how you respond when something goes wrong, right? Both implementing guidelines and policies as far as how you deal with an issue if it occurs, like a HIPAA violation, but also making sure that you respond promptly and undertake corrective action and document all of that. In all of its essence, that's what a compliance program is, right? It is implementing clear standards, enforcing those standards within your practice, even if it's just you. Then annually or throughout the year, assessing that to make sure it is up to date, that it's effective, keeping an eye on the laws for any new rules and regs, so on and so forth. Boiling it down in all of its simplicity, that's what a compliance program is.

Now, there are some really common pitfalls that happen, really regardless of different practice environment. We will really try to target this to the small and the solo practices since I know that that's probably the majority of you. One of the things worth highlighting is this term covered entity. There might be those of you that are operating in private practice and you don't accept insurances, you're not doing any billing whatsoever as far as insurance, everything is private pay. You are not technically considered to be a covered entity under the HIPAA Rules.

Doesn't mean that having a compliance program is a bad idea, it can still significantly limit your liability if there ever was an issue, but it just means that you're not actually at risk of being audited by the OCR. There actually are some protections given to covered entities, which we'll talk about a little bit later, neither here nor there, just wanted to be clear about what we are defining as a covered entity here and what the law defines it as.

Common pitfalls here, and let's say specifically those of you that are small or solo practices, one interesting thing that has really changed substantially in the landscape of compliance is that it used to be primarily the large hospital systems, the medical centers, the big groups in the insurance companies that were actually being audited and fined for HIPAA violations, and it really is not like that anymore.

The majority of the fines that are levied today, we'll talk about why this is in just a little bit, over 65% of all HIPAA fines in 2022 alone were levied to very small or solo practices. That is a new development, but primarily what we're seeing is that it's been causing this, again, I'll talk more about root causes in just a second, let's say what small practices are most commonly missing is really that more formalized compliance documentation.

Especially when you're a solo practice, this is an easy thing to not think about that much because it's just you, right? You know what you're doing on a daily basis, you

File name: GMT20231205-180008_Recording.cutfile.20231206140650565_1920x1080.mp4

know that you're not compromising anybody's information, but the issue is that especially in the behavioral and mental health space, if a patient, something happened and they filed a complaint against you, the government is going to audit you, and to them, it really doesn't matter what you're doing in practice, what matters is what you're able to prove on paper.

One of the first steps that we want you all thinking about is not what am I doing within my practice, but what do I actually have documented. What would I be able to prove that I'm doing in the event that the OCR was auditing me, either proof of risk assessment, proof of internal policy, proof of HIPAA training, business associate agreements. Missing risk assessment historically accounts for over 70% of all of the HIPAA fines that have ever been levied. That is a big one. If you've never completed a HIPAA risk assessment, there are ways you could do it for free.

You can even Google HHS Risk Assessment Tool through healthit.gov. They have a brand new risk assessment tool that you could utilize. I will say it's not the easiest thing. It's a free government resource but it can be a good starting point for you as far as getting a gauge on where you're at and what your needs are and just having that clear documentation in place to make sure. That's the key thing here. The biggest issue that we see in the very small practices that we work with is just lack of documentation, and that's what's going to be most important to the government. If it's not documented, it's not happening.

Now, there might be a bunch of you on here that have slightly larger practices, and usually in that type of an environment, once you're above 10 employees, there starts to be layers of complexity that gets added on top of this because you might have, let's say, a physical practice location or multiple. You have more employees, potentially turnover amongst those employees, and actually tracking those trainings every year becomes a little bit of a headache. Also, if you have policies in place, tracking the fact that your employees are actually reading those policies, another important thing.

Once you get to that size is when this really becomes important to implement some sort of tracking and management or monitoring mechanism. Picking one of your staff members in the practice to actually be responsible for this, to stay on top of it, to make sure that nothing is slipping through the cracks. That's usually when it starts to make sense as far as offloading some of those responsibilities from you.

Now, as far as formal documentation, we're going to look at some real-world case studies here, and by the way, we did not make these up. We redacted a lot of the information here just to protect the people that were fined. All HIPAA fines, though, are, not all of them, but there's the ones that are published that are fully public record, so you can go online and even look at some of the HIPAA fines that have been levied and just educate yourself.

There's one particular issue that the past several years has really brought about the particular issues that we've seen with smaller solo practices, and that is something called the right-of-access initiative. Right-of-access right now is the number one reason that people are getting fined, period, but particularly among smaller solo practices, especially in behavioral health environments. This is very common. The

File name: GMT20231205-180008_Recording.cutfile.20231206140650565_1920x1080.mp4

right-of-access initiative was an enforcement initiative of the OCR enforcing certain Privacy Rule positions that patients, if they request copies of their records from you, you are legally required to provide those records.

What often happens is, in all three of these cases that you see here, small solo practices, all the way up to, but still, all of these small practices, okay, fines range depending on how cooperative they were with the OCR's investigation, but what kicked off these investigations was very simply a patient requested copies of their records, the practice would not provide them, and that patient filed a complaint against them with the OCR. That is what led to all three of these fines. There's many more even than this. This is just to give a case study of this.

In general, within your practice, if somebody is requesting copies of their records, there's a couple of things that you want to keep in mind. Number one is this should be part of your internal policies and procedures. You have to have privacy policies that address right of access and how you respond if a patient requests copies of their records. You should be keeping a log of any of those requests. Then the third thing, and this is what's going to be most important for those of you that being in therapy-based environments, you want to be very cautious with your therapy notes.

What I mean by that is there are very specific provisions under the Privacy Rule that protect your therapy notes, meaning if a patient requests copies of their records, there are provisions in the Privacy Rule that state that you don't have to share your therapy notes with the patient. Other records, absolutely, but that only applies if you are clearly delineating your therapy notes from everything else.

Most behavioral health EHRs or EMRs or practice management softwares usually have a completely separate area where you're supposed to be logging your therapy notes. If you're not doing that right now, that is one of the first things that we highly recommend behavioral health practices start doing. Because if you're not separating those records, a patient could request information from you and you would legally be obligated to share all of your private notes if it's not clearly defined as therapy notes separately, so keep that in mind. If you want those notes to be protected, you need to track them that way. Those provisions in the Privacy Rule are set up to protect you. Make sure that you're taking advantage of that functionality within your softwares or EMRs, whatever it happens to be.

Now, 10 most common HIPAA violations. You can look through these. I'm going to focus on a handful just to talk for our conversation today. One of the biggest things that we see, and I referenced it before, is missing risk assessment documentation and something called corrective action plans or remediation plans. Under the HIPAA Rules, the security rules specifically, requires that you're doing a risk analysis. What they say is that this needs to be ongoing risk analysis in the practice.

Most people get away with doing an annual risk assessment where they document the review of your IT setup, your devices, your policies, your trainings, your vendors, right? That should be done at minimum once per year. You have the free tools available through Health and Human Services that can help you do that. Primarily, again, if you're looking to document your efforts, that's the easiest way to do it is just by documenting a risk assessment once per year because then you have all of that

File name: GMT20231205-180008_Recording.cutfile.20231206140650565_1920x1080.mp4

proof and a backlog of it if you're doing it every year on an annual basis and maintaining those records.

The third one I'll point out deals with vendors, and that's number five here. We talked about right of access already, but business associate agreements with your vendors is another really, really important area. Particularly, you might automatically have these with your practice management tools or with your EHR. One of the more common ones that we see in the behavioral health space is missing business associate agreements with your communication tools. Specifically things like your telehealth software, like let's say you've been using the free version of Zoom.

There were provisions passed during COVID allowing people to use non-compliant telehealth platforms like FaceTime or Zoom to provide therapy. Those protections no longer exist. That was ended earlier this year. If you are using a software like Zoom for treatment, you need to make sure that you have a signed business associate agreement in place with them. There's a ton of even free softwares out there that allow you to, that will sign a business associate agreement with you. We can make some of those recommendations if it's needed, but in the end, you want to make sure that you have a business associate agreement with all of those providers.

Device protections. Hopefully, if you're using a good EMR or a practice management tool, hopefully, all of your records are stored in there, and then you need to worry about your devices a little bit less. If you're storing things in your devices locally, making sure that they're encrypted. Then lastly, a lot of people get in trouble primarily because if there is a violation that occurs, there's something called the breach notification rule under HIPAA, which expects that you are responding and handling those breaches or issues properly.

That's super important because that's another way that you can get on the OCR's radar is if a breach or a violation occurs and it's not managed or tracked and documented appropriately. Usually, in the event that a violation happens, it needs to be reported to the government, depending on the number of patients that took place. We always recommend seeking legal advice for things like that if you have access to it, because that's going to be an area that you want to take seriously.

Now, we're going to get into talking about some benefits as far as why doing this is a good idea within your practices. There's a bunch of things that we can discuss here, but in general, what is HIPAA compliance all about? Number one, like we've spoken about, if you're doing that annual assessment, what that really allows you to do is potentially assess your risks and then hopefully actually fix them each year so that you're maintaining up-to-date policies and documentation and processes within your practice, which ultimately leads to a more standardized, well-run operation, meaning better quality patient service. Hopefully increased patient loyalty.

An interesting statistic that we see is that practices that are compliant and secure are on average 15% more profitable than ones that are not. Why is that? Really, that could be attributed to many, many different things, but primarily, there is this intangible quality of truly caring about protecting your patients' information. This is even something that I can sense when I speak with practices.

Let's say in the realm of moral and ethical responsibility, it is immediately clear to me when I speak with somebody that really genuinely cares about making sure that they are protecting their patient's information as much as they should be or as much as their patients deserve, and they are being proactive in making sure that they're staying on top of those things. That is something that I can sense very quickly, and I am telling you right now that is something that your patients feel from you too when you are engaging with them. It's one of the things that probably makes you good at your job is your genuine sense of care that you have for your patients.

One of the things that we talk to a lot of our practices about is that if you're taking compliance seriously and you're going through steps necessary to make sure that you are compliant, that your technology is secure, that you're doing what you need to be doing, that's something that you want to communicate to your patients, right? Even mentioning on your website that you only use HIPAA-compliant technology, talking to your patients when they're first coming on board with you, making sure that they understand those steps. Really what that does is it gives your patients a really clear sense that their data is being protected, and that just helps build trust and credibility right off the bat when you're initially engaging with somebody.

One of the funny things with that is a lot of people think about, so let's say you're protecting your patient's information. I'm trying to make this as specific as we can to the mental health space. One of the reasons why this is so important, especially in the mental and behavioral health category, is that if my dentist has a breach, let's say, I'm not that worried in the sense that there's not much that somebody could find out about me if my dentist has a breach. If my psychologist has a breach and all of the records of my sessions with them can be disclosed and put on the internet somewhere, then I'm really concerned.

One of the things, one of, I think, the really underrated steps that you could take within your practices to give your patients that sense of comfort is being open about what you're doing from a compliance and a security perspective to protect their data. That gives them a really, really clear sense that you are taking their information security seriously, builds that trust. At the end of the day, it just means that your patients, hopefully, their well-being as a result of what you're providing them and the services that they receive from you is much better outcomes, right?

Really, from a compliance perspective, one of the things that we talk about in all of the healthcare specialties that we work in is that compliance is really something that more than just preventing you from being liable, what it really does is it creates an environment where you're providing better patient care and better service to the people that you're working with. That is, again, that intangible quality of just truly caring, that's something that transposes into the care that you provide for your patients.

That culture, let's say, of patient safety, applies across the board, making sure that if you have people that are working for you, that that's a culture that you're developing within your practice so that your patients not only experience that feeling with you, with anybody that works for you, but also differentiating yourself. This ties in with what we were saying before about being open about what you're doing for compliance is a huge benefit to most practices.

File name: GMT20231205-180008_Recording.cutfile.20231206140650565_1920x1080.mp4

Discussing it on your website, discussing it with your patients, posting things in your notifications, disclaimers in your email, things that you could be clear about with them, and even saying no when patients are trying to communicate with you in ways that might not be compliant. All of that stuff helps build trust, right, and ultimately differentiates you from everybody else because it's not something that many people are going through all of those hoops for, so it's all really important.

Now, the last couple of things that I'll talk about here as far as benefits is there's an interesting thing under HIPAA where under HIPAA, if you are compliant with the HIPAA Rules, you actually can't be sued for privacy violations. Those enforcement initiatives are taken up by the government directly. There are no class action lawsuits or let's say individual liability issues that you need to be concerned about if you are a covered entity under HIPAA and you're fully HIPAA compliant.

That's one of the reasons that we recommend everybody take this seriously because if you have a clearly documented HIPAA compliance program, what winds up happening in your environment is that if there ever was an issue, it means that you have protection in the eyes of the law and it would be the government that investigates you rather than having to get stuck in a very sticky liability situation.

In order for that to apply, you need to be able to prove that you're doing what you need to be doing, assessing your risks, implementing policies, training anybody that works for you along with undergoing training for yourself, right? All of those things, you'll see significantly, significantly lower fines and smaller penalties to people that are not only being proactive about compliance but are also then in a position where they're cooperating with the OCR's investigations because you have nothing to hide them.

The last thing that we're going to wrap things up with here today, we're at the 30-minute mark. I usually try to keep these as far as me talking the 30 or 45 minutes if I can. We'll spend a bunch of time at the end as well for Q&A, so again, seriously, if there are questions that you have, take advantage of those Q&A features, we'll be circling back to everything at the end.

In terms of cost of noncompliance, there are some obvious ones and one of those things is financial, right? There are monetary penalties, there are HIPAA fines, there are also legal fees and issues that could result if you are found to be not compliant because then people do have the ability to create their own lawsuits against you. Those things are somewhat obvious. One of the less obvious ones is operational.

One of the things that we see, and it's one of the reasons why practices that are compliant and secure are more profitable than ones that are not, it's because going through that annual process of assessing yourself, updating your policies, revealing your risks, it creates an environment within your practice where you're quickly identifying operational issues or identifying areas where you could be more secure or even more efficient. That alone, operational efficiency is hugely important, but then operational disruption, if something goes wrong, is obviously a lot more significant.

There could be temporary suspension, revocation of your license. By implementing a compliance program, you're really ensuring that you don't have any of those

disruptions. There's no delay in your provision of patient care, no negative financial impacts, but also better patient outcomes. That's the next thing we wanted to talk about, which is in most cases, when a practice is audited by the OCR, or fined or there's a breach or a HIPAA issue, the primary damage that's incurred is not financial, it's often reputational.

Your reputation within the community that you serve is one of the most important things about you, right? As far as your ability to not only acquire new patients but continue to have the trust of the ones that you're serving currently. What we want to see all of our practices avoid is any type of reputational damage in the event of a HIPAA-related breach or a fine or whatever it is. There's then even things like legal fees, malpractice issues, negligence, any type of a lawsuit, right? It's just going to be time and money and so we want everybody to avoid that.

Again, our goal here for today to give you some key takeaways. Number one, you want to reduce your risk. Without, again, we don't want to scare anybody, but at the end of the day, you also need to be aware not only of what your responsibilities are, but what the risks that you face. At the end of the day, there is really not much that you would need to do to significantly limit your risk. Go online, use that free tool for risk assessment. Look at your policies. If your policies were implemented more than three or four years ago and you have not updated them recently, look into acquiring or developing new policies. That's the second thing.

Make sure that you've undergone HIPAA training, right? That you have business associate agreements with those vendors. That's like four steps, risk assessment, policy training, and BAAs. That will significantly reduce your risk of being audited, of being fined, of having a liability issue. Ultimately, the downstream impact of that is hopefully a better patient experience for the people that you're serving. Again, a good compliance program just creates a standardized operation resulting in a much better experience and better patient outcomes in the end, and hopefully improved profitability.

The little bit of time that you spend focusing on compliance, so the little bit of money that you invest to set up these things within your practice really, really goes a long way in just making sure that your patients are being protected, that your risk is being reduced, but also that you're running a more profitable practice is the goal of all of this. With that said, at this point in time, I can go ahead and dive into maybe some of the questions that we received, both before the webinar and live today. I am going to open up some of these questions here. I can load them up.

One of the questions that we received, we received two questions before the webinar, and one was on do text messages violate HIPAA. Then the second one is managing HIPAA and privacy with third-party apps for mental health and safety plans. Text messaging your patients is usually considered to be problematic. There are ways that it can be done in a way that's compliant. First thing I'll say is you should always have your patients sign an electronic communication consent form, both a form that allows you to text them, but also a form that allows you to email them in a way, let's say, that is compliant.

By having them sign those consent forms, even if you're doing it in a potentially non-compliant way, does limit your liability quite a bit. Even outside of that, once you're having them sign those forms, it's a really good idea. There are actually HIPAA-compliant text messaging tools that you could purchase for your practice, even ones that will integrate into your EMR or your practice management tool, so that you have the ability to do two-way text messaging with your patients in a fully HIPAA-compliant way, negating any issues. They will sign a business associate agreement with you.

That's one of the biggest issues is that from a text messaging perspective, like iMessage, WhatsApp, Facebook Messenger, none of those companies will sign a business associate agreement with you. Even if your patients are consenting, you could still be liable because the law requires you to have BAAs with those companies. Finding one that will sign a BAA, leveraging that instead of just your personal cell phone, right, making sure that you're approaching it that way could be a really good idea.

That applies to almost everything concerning applications, right? Things like email, making sure that if you're on like a Gmail or an Outlook, that you have a business associate agreement with Google or Microsoft. Sometimes you need to be on the paid business version of those things, but all of those different third-party apps very commonly are happy to sign a business associate agreement with you. You might need to pay for that upgrade, but it's usually well worthwhile just to give you that peace of mind, make sure that you're where you need to be.

Another question we got was, how does HIPAA relate to 42 CFR Part 2? This is probably going to apply to those of you that are in the slightly larger practice category because in order for you to fall under 42 CFR, you have to be a federally funded substance abuse treatment facility. That's really the primary connecting factor. Both 42 CFR and HIPAA are regulations published by Health and Human Services. HIPAA deals with general patient privacy and security. 42 CFR deals very, very hyper-specifically with SUD. Substance Use Disorder Treatment Facilities and things like that. That's the primary area of overlap. You need to comply with both if you're a substance abuse treatment facility.

The last question I'll cover on the ones that we received prior to the webinar. BAA requirements and authorized video platforms. *Psychology Today* offers one, for example. Any video platform that you're using as far as back-and-forth engagement with your patients, you want to have them sign a business associate agreement. Again, there's lots of free ones as far as the video platforms that are out there. There's lots of ways and opportunities you could do this. The thing that matters most is that you either sign their BAA or that they sign yours. If that's not a possibility, there is no possibility of you using that platform in a way that's compliant, so really worth looking into there.

All right, so those were some of the questions that we received prior. Robin, do we have any questions that were asked live in the webinar here that I could tackle before we finish this out today?

Robin: Yes. Oh, just reiterating, definitely if you have questions, please submit them using the Q&A box at the bottom of the screen for most people in Zoom. We're

File name: GMT20231205-180008_Recording.cutfile.20231206140650565_1920x1080.mp4

taking questions now. The one we have, someone was asking if you could just revisit your point about when an independent practitioner or small practice is not considered a covered entity. Is that because they don't bill electronically or for another reason?

Liam: Yes, so in order for somebody to be considered a covered entity, you have to be processing what's called a covered transaction. In this case, an insurance claim. If you do not accept any insurances and you're not doing those, it could be electronic or otherwise, doesn't really matter. If you are accepting insurance and applying for reimbursement, you're a covered entity.

The way that HIPAA worked is originally in 1996 when HIPAA was passed, the only people that were covered under HIPAA was the actual insurance companies. There was then additions made to the Privacy Rule, which then said you're a covered entity, not only if you're a health insurance company, but if you're billing through a health insurance company because you have access to all of the same data as a healthcare provider. There was then another rule passed under HIPAA called Omnibus, which said, if you are engaging with any of those covered entities as a business associate and they're sharing patient information with you, you also need to be HIPAA compliant.

It's really following that stream down from the insurance companies to your practice and then to the vendors that you're working with. That is what would make you a covered entity along with any of the vendors who are using a business associate. Hopefully, that makes sense.

Robin: Awesome, thank you. Deborah just asked if it would be possible to see an example of solo practice compliance document.

Liam: It depends on what you mean by compliance documents, right? If you're referring to policies, one of the funny things with HIPAA is that the policies is just what the law requires, right? In most scenarios, your policies that you have in place will be the same as what anybody else would need. What's different is for every policy, there's an accompanying procedure. That's why you commonly hear those lumped together, policy and procedure. I'm embellishing on this just to be very, very clear. The policy is what the law requires, the procedure is how you implement it.

In terms of the policies that you need to have, you can review the HIPAA regulations and just mirror the policies to that, but then have an accompanying procedure that just explains in your environment, this is how we implement and operationalize this policy. What I will say as we're nearing the end here, if there are those of you that are on here that are looking for a potentially easier way to address these things, part of what we do here at Compliancy Group, and we are the APA's preferred provider of HIPAA compliance solutions, we have a software platform that is almost like having QuickBooks, but for compliance, or TurboTax, but for compliance, so that you can go through your risk assessment.

It automatically generates policies and all of your forms and all of your trainings and business associate agreements for you. That's a very simple explanation of it, but it's essentially just designed to walk you step-by-step through everything that the law

requires. If you would like to learn more about that, I am sending a link to our landing page with the APA. You can go ahead and jump on that site and request information. Feel free to schedule a demo of our platform, or you can request a quote. We'd be happy to speak with anybody. That's part of the service that we provide. You get a discount on it as an APA member, which is great. Robin, do we have any other questions?

Robin: I'm looking, I think that was everything. You must've done such a good job with your presentation. I'm not seeing any more questions come through, so folks, if you have any, we'll give it about 30 more seconds, but thank you so much for your time and for joining us, Liam. We want to thank you to everyone on the line for your participation today. Also thank you to Compliancy Group for making today's webinar possible.

We will send out a recording in about two weeks, and that recording email will also include a copy of the presentation slides. A certificate of attendance will be issued to those who have watched for a minimum of 45 minutes today. That is not a CE, it is a certificate of attendance. We have, hold on, oh, you got it, Liam. With that, I think we are done for today. As soon as this webinar has ended, a short survey will appear on your screen. We ask that you please take that survey and give us your feedback so we can continue to improve our webinar program. With that, thank you, everybody. Thank you, Liam, again. We hope you all have a wonderful rest of your day.

Liam: Thanks, everybody. Thanks for having me again.

[00:45:44] [END OF AUDIO]