

Title: Compliance and Security: Why You Need Both to Be HIPAA Compliant
Date & Time: February 28, 2024 at 1pm ET

Moderator: Hello, and welcome to today's webinar, Compliance and Security, why you need both to be HIPAA compliant. 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 the 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 or its editorial staff. Email advertising at apa.org to learn more.

Next, the 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 the presentation will be emailed to everyone in two weeks' time. The recording will include the presentation slides. During our time together, you will be on mute. You can communicate using the Q&A box located on your webinar screen. Have a question for our presenters, type them in using the Q&A box located on your webinar screen. A link to the presentation slides will be posted in the chat box of your webinar screen. If you miss them, don't worry. We'll email them to you with the recording.

Now, let me introduce our presenter, Liam Degnan. Liam Degnan has eight-plus years of experience combining risk management, SAAS sales, and regulatory compliance in the healthcare space. As Compliancy Group's Senior Sales Manager, 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 Degnan.

Liam Degnan: Hey, everybody. Thank you so much for having me. I really appreciate it and looking forward to this. I think that to give a little bit of a very, very quick lay of the land as far as just some of what we're going to be going through, particularly, so not only just compliance, but when you talk about things like cybersecurity, it's especially common among solo practices, and I would say, let's say, very small practices just in general.

The idea of IT and cybersecurity is extremely nebulous and somewhat difficult to actually process and understand in a way that's meaningful because in your environments, the majority of you did not go into the business of becoming compliance or security professionals. You went into the business of psychology and of helping your clientele and helping the people that you serve. Our goal for today is to break this down in a way that is hopefully really, really practical, and particularly

the topic of cybersecurity. People think of this in an often extremely advanced technical way, and I don't think it really needs to be that way.

Some of what we're going to be talking about and what you'll see as we go through is that the majority of the ways that you can limit your risk and make your practice more secure is often not even, let's say, from a technical perspective or from an IT perspective, it's more so just about how you operate as a practice, educating yourself in a more effective way, but also anybody that could potentially work for you if you have staff, administrative employees, or if you are a provider group.

We're going to be going through some of those different dynamics today. To start, we're going to be talking and going through just a general introduction to HIPAA compliance. We'll then be going a little bit deeper into some of the specifics as far as key areas of risk for very small and solo practices from a security perspective. Let's say industry-wide today, what are the things that you really should be thinking about within your practices and how can you mitigate those risks?

As we go through to the end, it's really my pleasure to help address any questions that you might be bringing to the webinar today. It could be compliance-related, security-related, whatever it is, I'm happy to discuss it and have a free-flowing discussion here. My goal is, like I said right at the beginning, is for most of you, I know that in starting your own practices, these are probably not things that you even really want to be thinking about. The majority of you are probably just focused on providing a great service and helping the people that you serve.

Our goal is hopefully to break this down in a way that makes it as simple as possible so that you have an easier time managing it and can focus on your practice, growing your practice and helping the people that you serve. With all that said, what I'd like to do is just give a very quick breakdown as far as some compliance basics. One of those things is just, foundationally, who actually needs to be HIPAA compliant and who does this apply to?

It's an important thing to call out because I know that there are probably many of you on the webinar today that are private pay. As far as HIPAA is concerned specifically, there are really only two buckets that you could fall into as far as the HIPAA rules are concerned. One is what's called a covered entity, which is anybody that is not only treating patients, as the government deems it, but is also billing insurance for those services.

When we talk about the formal definition of a covered entity under HIPAA, as far as the HIPAA rules are concerned, it's really primarily regulating those of you that are billing insurance because in order for something to be considered PHI or protected health information under the HIPAA rules, it has to be connected to what's called a covered transaction, in this case being an insurance claim. That doesn't mean though that those of you that maybe are not billing insurance should still not have a compliance program.

One of the unusual things that is not often talked about is that when you are a covered entity, there's specific clauses under HIPAA that provide additional

protections to covered entities that prevent private right of action, let's say. Meaning if you ever had a breach or an issue or there was a HIPAA violation within your practice, your patients can't sue you if you're a covered entity, they have to report you to the government and it would then be the government that investigates and levies a penalty if they choose to.

If you are not a covered entity, those same protections don't really exist, so in order to limit your liability, it's still a really good idea to make sure that you're taking things like privacy and security seriously, looking at these things within your practice, because in the event that there was a liability issue, you of course have insurance. Above and beyond that, things like cyber issues are often not covered under general liability insurance policies. I bring it up because it is a good consideration just to be thinking about, but also want to be really clear about who on the webinar today would actually be covered under the HIPAA rules and formally considered a covered entity.

Now, the second one is something called a business associate. More than likely, this is something that you are all familiar with. If you're using, let's say, an EMR platform or a practice management tool, or maybe your telehealth platform, you have signed business associate agreements in the past. Hopefully, if you're using those tools, you have business associate agreements with them. If you don't, you may have signed agreements with them. We could talk more about that. One of the things that makes somebody a business associate is that they obviously are not treating patients, but they are providing a service to covered entities that involves them having access to patient data.

One of the most foundational responsibilities that you have as a covered entity is that if you're working with a vendor, you should have a signed business associate agreement in place with anybody that is accessing your patient information. One of the reasons the government requires this is because otherwise it's sort of just a free-for-all. If that requirement wasn't there, you could share patient information with anybody without any real limitations, especially vendor relationships.

It nowadays, especially in as many cloud-based environments as we have, a significant percentage of the breaches and violations that happen in healthcare are at the fault of a vendor, so good to understand those definitions. Think about what are the platforms that you're using internally? What are the different tools, the vendors that you're working with? Do you have those things in place if they could be potentially touching your patient's information?

Now, aside from just who needs to be HIPAA compliant, if you've been on any of our webinars before, you've heard us talk about something called the seven fundamental elements of an effective compliance program. This does not come from us. This is a very, very pervasive document in all of healthcare compliance. It comes directly from Health and Human Services, as well as the Office of Inspector General. Essentially, what they define as being the boilerplate requirement of a compliance program, and this could be HIPAA, Medicare, state regulations, doesn't really matter what it is. This is the end-all be-all as far as the government is concerned. We'll talk more about the specific requirements as we go through this in just a little bit, but one of the things

that I always like to bring up before we even talk about specific requirements is just this word, effective. Especially those of you that are on the webinar today that are very small practices. HIPAA can be uniquely challenging because all of these rules and regulations are written in a way that is almost intentionally vague because they have to apply to you, same as it applies to much larger group practices, same as it applies to business associates like Amazon and Microsoft and Google, along with the largest hospitals and health plans in the country.

The law does not differentiate whether you are a small practice, a large hospital, an insurance company, doesn't matter who you are or what you do. If you are a covered entity or a business associate, you are legally required to have an effective compliance program, but that doesn't mean that it's always going to look the same.

Part of the reason for that broadness and that almost intentional vagueness in these regulations is that in the eyes of the government, they don't want this to be just a check off of a box, they want you to understand these guidelines and implement them to your practice in a way that makes sense for you because what is effective for you as a very small practice is maybe not going to be the same as what's effective for a really large hospital obviously. What's effective for you might not even be effective for the practice that's up the road.

How do you actually figure out what that is? How do you identify what's effective for you and how do you prioritize these things within your practice in a way that allows you to really begin to understand this and set this up properly? To get into that a little bit, I'll give a little bit of an understanding as far as the HIPAA rules are concerned. There are four HIPAA rules in total, privacy, security, something called an omnibus, which also contains another rule called breach notification.

The privacy rule is relatively straightforward. These are standards of policies that you should have in your practice, essentially concerning use of disclosures. When can you disclose a patient's information to somebody else and when can't you? Not too complicated. The omnibus rule in a similar way, you have to have business associate agreements with vendors and you need to report breaches if they occur. Relatively straightforward. There is some complexity there if you ever had a breach, but not too complicated.

The security rule, and part of why the topic today is so important is because it tends to be the security rule where a lot of people get tripped up, especially as it concerns making this relevant in your practice environment. One of the things that HIPAA requires is the completion of something called a security risk assessment.

A lot of people think about the security risk assessment as being primarily a technical component and sometimes it is, like a review of your IT setup, your devices, your network, your Wi-Fi, your firewall, all of that stuff, but the funny thing is that the risk assessment for HIPAA in its entirety, outside of just dealing with technical security, also covers what's called administrative requirements, which is policies, procedures, trainings, documentation.

The day-to-day operations of your practice, let's say, and it's a good thing to talk about because among, let's say historically, across the board, in the history of HIPAA compliance, roughly 70% of all of the HIPAA fines that have ever been levied referenced missing risk assessment documentation as a key reason for the fine. If you have never completed a HIPAA risk assessment in your practice, it's always where I recommend beginning because one of the benefits of it is not only will you be satisfying that requirement to complete a risk assessment, which protects you, it actually gives you really good insight into what you should actually be thinking about in your practice.

If you never do a risk assessment, you'll never really know what you should be thinking about from an IT perspective or for your policies, your procedures, trainings, things of that nature, all of which are required. By going through that assessment process, it goes a long way in helping you identify what you actually need and then can address those needs in a way that is effective for your practice. All of this is about good faith effort.

In the eyes of the government, I hate to say it this way, but it's not about what you're doing in practice, it's about what you're able to prove on paper, so going through that assessment, documenting your efforts, making sure that you're able to prove that you address these things, but doing it in a way that makes sense for your business is really how you protect yourself as far as the law is concerned.

One of the funny things is overall, it's an unexpected benefit that we see with a lot of the practices that we work with is that your patients generally know and can tell when you really care about these things. Practices that are compliant and secure are on average 15% more profitable than ones that aren't, not only because it mitigates risk, but also because it helps you build trust and establish additional credibility with your patients that might not otherwise be there.

I think that it is a huge part of the patient experience, especially when you are providing behavioral and mental health services, trust goes so, so far and really understanding your needs from a compliance and security perspective, but even just within your practice, really caring about protecting your patient's information and making sure that they feel comfortable with you in that regard goes a long way.

Just to highlight this, there are some statistics. You could see the reference here from the NIH, but 68% of patients would say that they are not confident that their healthcare provider protects their medical records. Imagine how much comfortable your clients would feel with you if that was zero. Among people that experienced identity theft, 53% of them said that they believe that their provider's negligence caused or contributed to identity theft. Because it's very rare, especially if you're billing insurance, you have some very high-risk data there as part of that process, there's very few, let's say, service providers, period. Even banks might not have as much information about your patients as you do.

That's why healthcare organizations are often more at risk for things like ransomware, phishing scams, cyber attacks. We'll talk more about that in just a little bit, but I bring it up because it's an important thing to highlight. It's more than just

about protecting your practice, it's about actually serving your patients, providing a better quality service to your patients and clients is what this is all about.

With all of that said, I'd like to give that as a little bit of a backdrop, just to give a few foundational items as far as compliance is concerned. We're going to talk about some of the differences between compliance and security now and go through some of the key areas of risk that currently are facing small practices. Again, I know that it's been stated already, but if you have questions, please ask those questions as we're going through. We will be circling back at the end. I'll do my best to make sure we get everything answered before we're done here today. If we're not, you can always just email me. I'm happy to help. There we go.

Compliance versus security. Compliance is primarily about your ability to prove that you are satisfying the law. It tends to be a black and white sort of a thing. There's no such thing really as being mostly compliant or partially compliant. You're either doing these things or you're not, and you either have the ability to prove that you're doing these things or you don't. Security is a little bit different because everybody has a different risk profile. There's a lot of shades of gray. Every practice is going to have different areas of risk. The idea of being secure is a little bit more nebulous as compared to being compliant, but really both are necessary.

Security within your practice, understanding the risks that you face, but also making sure that you're documenting your efforts in a way that you're able to prove these things. Both are really important. Now, the whole concept of security, when we talk about, a lot of people think about their firewall, encryption, backup, antivirus, anti-spam, malware, all of that sort of stuff, at the end of the day, what does it mean to be secure? What is security?

You'll see the dictionary definition as being more outlined around freedom from danger, safety, freedom from fear or anxiety. I think that's a really good one because for those of you that maybe think about your practice a lot and think about the risks that face your business, and these are things that I understand as well, thinking about security less about what technology do I need to implement and more about what do I need to do in my business to make sure that I don't have any fear or anxiety about how things are going to shake out is a healthy way to approach it. Because if you're able to think about it in that way and just identify the areas that are key areas of risk for you that keep you up at night, and you can identify some reasonable strategies of addressing those things, it goes a long way in just giving you peace of mind, but then also protecting the business as a whole. A lot of that then comes down as well to the importance of trust. This circles back to your patient's experience with you.

20% of patients are lost by a practice annually on average. Only 68% of appointments within most healthcare practices come from existing patients. 83% of patients say that they would recommend a practice that they trust, just if they trust you. Nothing having to do with the quality of the service that you're providing, purely just based on trust. Most people say that they would stick with a practice that they trust, but we live in a predominantly digital world and with that, there are some

inherent risks, so 62% of patients want to communicate with their providers through email.

64% of patients want to be able to schedule online. 61% of patients say that digital services are important when they're choosing a provider. This is one of the most interesting ones to me. Two out of three patients would switch providers entirely just to be able to have access to their information online as compared to paper records. Along with this, there's unfortunately a lot of bad news within the space. There's tons of medical records that are breached per day. Most healthcare organizations have had a breach of some kind, even just in the last two years. 86% of those mistakes and the breaches that happen are due to administrative error.

I bring that up specifically because it's a really good tie-in to what we're going to talk about as far as cybersecurity basics and how you can actually protect your practice. When we talk about administrative errors, in thinking about the technical components of security, most people think about technology, but really the number one way that you can mitigate your risk from a cybersecurity perspective, it's actually by through training and through very clear policy.

You can have all of the security in the world. Your laptop could be encrypted. You could have secure email. You could have antivirus, anti-malware, a strong firewall, all of these things, but if you're not aware of basic things, like even phishing scams, if you don't know how to recognize a phishing scam, or if you have employees and you haven't trained your employees on how to beware of a phishing scam, and they could be clicking on suspicious links in an email that is sent to them, or putting their credentials into something that they're not supposed to, it does not matter how much technical security that you have. If people are making mistakes like that, none of it matters.

When we talk about practical, simple ways of mitigating your risk from a cybersecurity perspective, a lot of it really comes down to policies, procedures, and training. One of the reasons why this is important to care about, on average, and let's say this is healthcare organizations as a whole, we'll make this even more specific to private practices, but more than one in 10 sensitive files are open to every employee. If you have employees in a small practice, it's usually even much more than that. Most of your employees could probably access all of your patient's information if they have access to your EMR.

The average cost of a data breach in the healthcare sector was \$4.45 million in 2023. Over 50% of organizations have more than 1,000 files open to every employee. If you have an established practice, and you've been around for a long time, you probably have, it could be 1,000, it could be a little bit less, it could be a little bit more, at least a couple hundred patients in your database with files that are accessible either to the people that work with you or just to yourself.

Among all of those data breaches, let's say among small practices specifically, 90% of them are storing patient information digitally. 48% of large providers say they've experienced a breach in the past. One in four small practices say that they have. 46% of small practices said human error, again, was the leading because of a data

breach. The healthcare industry as a whole is very, very high risk for this and there's a lot of reasons for that.

One of the reasons is, we talked about this a little bit earlier, you have really valuable information, especially if you're billing insurance within your practice, one single healthcare record could be sold in the black market for anywhere between 5 and 10 times more than a debit or credit card number. Reason being is because that information could be used for anything, from identity theft to blackmail. If somebody takes a debit card, they can get a quick transaction before it's flagged, but if somebody gets healthcare records, they could use that data for a lot, a lot of different things.

One of the most common areas of attack right now among small practices is ransomware. You'll see the book definition here, but the basic way that you can understand ransomware is let's say that you get an email and it seems like it's coming from your EMR. It tells you, "Hey, we identified an issue. Please click this link to log in so that we can address it." Then you click on that link. You think that you're logging into your EMR. Instead, you have now provided your credentials to a cyber predator, basically.

What those cyber predators will do is they will get access to your system, your network, your EMR, and they will encrypt all of that data and set a ransom on it, and they'll tell you, "You have to pay us \$10,000 or you'll never get access. You'll never get your access to the system again." A lot of people fall victim to this. It is especially common in healthcare because there are so many small to mid-sized practices.

It's rare for a large hospital system, let's say, or a health plan, they have very advanced security, you need to be a very advanced cyber predator to break into those organizations, so a lot of, let's say, the bottom feeding cyber predators are going after the small practices because you have very valuable information and you're sometimes vulnerable. From a healthcare perspective, and especially in behavioral health because of the level of information of access that you have, these are important considerations, but there's a few things that we could talk about.

Some of the most common sources of violations could be phishing scams is what's most common nowadays. Also, lost and stolen devices is another big one, especially if you have a physical office or files stored locally, could be a vendor of yours gets hacked, could be actual theft, things like that, but most of the time, the technology is not the problem, and I'm going to keep coming back to this. 86% of even IT related incidents occur as a result of administrative error. Some of the number one ways that you'll see people are able to mitigate their risk is just by going through cybersecurity training.

This is a requirement of HIPAA. Even if you're a solo practice, at least once per year, you should be undergoing a privacy training and incident management training and a cybersecurity training that deals with the most up-to-date information in the industry today. You'll even see here why this is so important. Almost 90% of the people that were victims of ransomware attacks had anti-malware and antivirus software installed. 75% of them had email spam filters. 20% roughly had ad and pop-up

blockers. Only roughly 14% of them had done cybersecurity training. More than any of these things, training is one of the number one ways that you can mitigate those areas of risk.

One of the funny things is the other thing that you can consider is really strong backup systems. If you're using an EMR, you might have this automatically. If you don't, it's something to really consider, but if you have a backup solution where all of your patient's information is stored, what that means is two things, even if you fall victim to a ransomware attack, you won't need to pay the ransom because all of your patient's information is already backed up somewhere, so you can shut down your system, turn on your backup, and get back up and running very quickly, and that's a really great recovery strategy.

Then the number two thing is employee training. If you're going through those trainings, preventing these things from happening in the first place, but then you have really strong backups system and disaster recovery plan, those two things are actually required under the HIPAA rules to begin with. Those are things that should probably already exist in your practice anyway. Just by doing those two things, you can mitigate the overwhelming majority of the cyber risk that is facing your practice. Other things worth talking about, you could talk about encryption, making sure that your devices are encrypted.

There are some basic strategies you can implement for that. Implementing a more advanced firewall, network security, all of that stuff is great, but if all that you do and all that you get out of these webinars is, "Hey, to make my practice more secure, I need to figure out how I'm actually backing up all of my patients' information and I need to make sure that I'm going through a really good training on what are the modern day risks. How can I recognize a phishing scam? How do I prevent ransomware?" Just those two things will get you a long, long way of the way of where you need to be to creating a much more secure practice, so really worth highlighting.

One of the things to bring up, so you'll see a lot of larger fines here to larger healthcare organizations. I want to talk actually about some of these smaller fines that have been levied because within the behavioral health space right now, there's something that has been happening called the right of access initiative. For those of you that are covered entities, the number one way that very, very small practices currently today are being fined is not necessarily even due to security related issues, it's due to privacy violations where a patient requests copies of their records and you don't supply them.

I'm talking about this along the topic of security because it is an area of risk. There's been a lot of practices that have been fined for right of access issues. Aside from cyber predators, you want to make sure that you're mitigating these risks in the practice and this is a super, super easy one. You could see some of these fines, \$25,000, \$70,000, \$15,000. There was a solo practice right where I am in Long Island that was fined a \$100,000 because they were completely ignoring all of the OCRs increase and not replying to them. The OCR is the enforcement body of HIPAA.

In all of these cases, these practices were fined simply because a patient was requesting copies of their records and the practice was not providing them. Make sure in your practice, this is another great way to mitigate your risk today, make sure that you have something called a right of access privacy policy and that you have a well-defined process for how you respond to patients if they request copies of their medical records.

This doesn't mean that you need to share all of your therapy notes with them. Psychotherapy notes specifically have protections under the privacy rule, so you do not need to share those things with your patients if they request them, but it's often difficult to differentiate between the two. That's why most EMRs have a separate section in them. If you're using therapy notes or simple practice tools like that, they have dedicated sections in those platforms for you to keep tabs on your therapy notes. Otherwise, everything is disclosable if a patient requests it.

Again, this is a really easy one, just make sure that you have a right of access policy and make sure that you get back to your patients within 30 days if they request copies of their medical records. This is something that the government is enforcing very heavily right now. It is the number one way that small practices are getting fined. It is the number one source of HIPAA fines for the last two years or so. Previously, it used to be risk assessment. Now it is this. If all that you get out of today is you need to implement a strong backup, go through cybersecurity training, and implement your right of access policy, you're probably doing really pretty good.

Now, other areas to talk about as far as HIPAA compliance is concerned as a whole, overall, HIPAA compliance requires you're doing that assessment. For those of you where a lot of this is new, you're not familiar, you're trying to figure out where to begin, going through that HIPAA risk assessment process is a great, great way to start. That'll help you identify the policies that you should have in place the trainings that you should be going through, what you might want to consider from an IT perspective, and you'll see it really connects all of these other dots, training, policies, encryption, backup, disaster planning.

This is something that you can even test within your practice. Really think about if I was a victim of a ransomware attack, how long would it take me to get back up and running following that type of an attack. Right now, you can consider overall just getting HIPAA compliant, updating your passwords, keeping everything up to date in your practice, train yourself and your people on what to look for all of these things, and look just overall what we've covered today. Again, it's not complicated, folks. Cybersecurity does not need to be difficult. You can make this very, very simple and these are just some really great, powerful ways to protect your practice.

If you're looking for an easier way to manage these sorts of things, we would love to chat with you here at Compliancy Group. Our platform is designed to handle the overwhelming majority of the HIPAA requirements, including assessment, policy, and training so feel free to contact us if you'd like to learn more about that, but otherwise, we'd love to tackle some questions and I'll be as helpful as I can while I'm here.

Moderator: Brilliant. Thank you, Liam. One question we have from the audience is, what tools do you recommend for those in private practice and/or practicing teletherapy?

Liam: If you're practicing specifically teletherapy, there's tons of tools that you could use, specifically telehealth platforms that you could use in that process. The one thing that you want to keep in mind is you can use realistically any virtual meeting platform as long as they are willing to sign a business associate agreement. That's like the litmus test. Even Zoom. Zoom can be HIPAA compliant, but it's not out of the box, so if you're using like the free or the light version of Zoom, it's not going to be HIPAA compliant.

You need to upgrade in order for them to sign a business agreement with you, but there are really affordable telehealth solutions that also will just sign a BAA out of the box, and those are fine, so that can be worth considering. Those are the types of tools. Use whatever you like, just make sure that they're signing a business associate agreement.

Moderator: Awesome. Another question we have is, I was wondering if Google Workspace or Microsoft Outlook are HIPAA compliant?

Liam: It's in some ways the same answer. Google Workspace and Microsoft Outlook are not going to be compliant out of the box, but it's not expensive to make them compliant. In the case of Google and Microsoft, they have HIPAA compliant tiers that you can upgrade to, which makes the entire workspace compliant. In the case of Google Workspace, that means that you could use Gmail, Google Sheets, Google Forms, all of those things in a compliant and encrypted way, and it's as simple as just doing that upgrade and signing the business associate agreement.

Compliance with things like email becomes a little bit more complicated because when you upgrade with Google Workspace, it means that the way that the emails are stored is compliant, but not the way that you're sending them. In order for emails that you're sending to be compliant and encrypted, you would need to use an actual email encryption tool. The one that I recommend for this most often is a company called Paubox. That's P-A-U-B-O-X. They have great solutions and they are super, super affordable. It's also really easy to use.

A lot of people have negative experiences with email encryption because it's like a portal that they need to log into and then they do multi-factor authentication. Pawbox is seamless email encryption. It encrypts it as they go into the client's inbox. There's no portals that they need to use. It is super simple. That's always what I recommend.

Moderator: The question we've had a few repeats of are, where do you find a HIPAA risk assessment? Is there a protocol or program?

Liam: Yes. The government I know just released an updated risk assessment template, so to speak. Even if you Google HHS risk assessment online, it'll take you to their free healthit.gov risk assessment tool. Just keep in mind that it's a government resource so it's not going to be like the most plain English, easiest to

use type of a thing, but it can be a good place to start. If you're looking to complete a risk assessment on your own, a tool like that could be a great place to begin.

Moderator: We've had someone else ask if QuickBooks is safe to use.

Liam: There's two iterations of QuickBooks. There is the QuickBooks that you could actually download locally on your computer, which does not connect to the cloud. That, believe it or not, is compliant, provided that your laptop is encrypted and secure and in the way that you're using it, it's compliant because QuickBooks does not then directly have access to that data. It is all just local on your computer.

The cloud-based QuickBooks platform, if you're using it like directly through their website, is typically not compliant and they're usually not willing to sign a business associate agreement so that is not a tool that we usually recommend for client invoicing. Now, the one thing to keep in mind here though is QuickBooks is a secure payment platform. Just because they're not HIPAA compliant does not mean that it's not secure.

Most of the time, if you're using QuickBooks, it's because you might be in private practice and those clients that you're billing through QuickBooks are private pay. Those are not covered transactions under HIPAA anyway. You wouldn't really need to be worried about those. It's only the patients that you are billing through insurance that you need to be concerned about primarily, specifically as far as HIPAA is concerned.

Moderator: Wonderful. Thank you. Another question asks, is there a way to manage patient's ability to record their session and how does this affect liability?

Liam: That is a good question. At the end of the day, if a patient chooses to record their sessions without your permission, there's not a ton that you could do about that. As far as the legality of that and things of that nature, it's hard to tell. Usually, if it's a virtual meeting, it would most likely be against the law for them to be recording that phone call or that session without your permission, but if it's an in-person meeting, there's not much preventing them from doing that, so I wouldn't necessarily be concerned about it from a liability perspective.

You want to just always make sure that you're above code anyway. In all of your interactions with your patients, them recording you hopefully shouldn't be much of an issue as long as you're staying above board and that's the goal.

Moderator: Another question asks, how does this change when you work from home or how does compliance look in a solo private practice?

Liam: Work from home is an interesting one because even among the practices that we work with, it's very, very common for people to be working from home. A lot of digital health companies, even with hundreds of employees, everybody's working from home. The requirements in some ways are very, very similar. It just depends on how patient data can be accessed. If it's in your home and you're storing paper records in your home, those should be in a secure file cabinet. If the only access to

patient records is through your EMR, it's a lot less concerning and you could just make sure that you have a strong and secure password on your EMR.

If you have things on your devices, that device should be encrypted, password protected, shouldn't be left lying around, basic things like that. It's more procedural and operational, even than it is concerning the security of it directly but HIPAA has no issues with work from home environments whatsoever, just as long as you're following the right processes and securing patient data.

Moderator: Wonderful. Someone else asks, can encryption be automated in Outlook?

Liam: It depends on what you mean by can encryption be automated. Usually encryption is something that you just turn on or turn off. In Outlook, there are encryption settings you could turn on and then, yes, you could just leave it and forget it. Again, keep in mind that doesn't mean that the emails that you're sending are encrypted. Emails that you're sending have to be encrypted separately, which you can do through Microsoft, or you could purchase a standalone email encryption service, which is sometimes what I recommend because they just work a lot better and are a lot smoother.

Moderator: Another question asks, if your clients submit on their own to insurance, does that mean you're not a covered entity?

Liam: Yes, yes, if your clients are taking the bill that you give them and then seeking reimbursement on their own, that means you are not a covered entity. Again, keep in mind that when you are a covered entity, it actually gives you some additional protections, so still not a bad idea to take these compliance requirements into consideration, but you would not be considered a formal entity under the HIPAA rules. You would not be directly audited by HIPAA, even if something was to happen, it would be a private liability issue.

Moderator: Someone else asks, what about payment methods? I've been told Zelle is not HIPAA compliant.

Liam: Zelle is not, yes. Things like Zelle, Venmo, but it goes back to the QuickBooks example. If those are private pay clients, it's not as much of an issue as long as they are okay and have consented to providing you with payment through those means. If that is an insurance-based customer, if that is an insurance-based customer, you really shouldn't be accepting payment through those types of platforms. Let's say things like copays and otherwise shouldn't be accepted through there.

Moderator: We have another question that asks, what risk is there using the USPS for billing and sending other information?

Liam: Absolutely none. USPS is considered a conduit which gives them specific exclusions under the HIPAA rules. They have all of their own requirements that they need to follow and abide by so there is no issue with using USPS, FedEx, UPS. They all have exclusions under HIPAA. If you're sending client invoices or letters, mailings, that is totally fine. The only thing to be wary of is marketing. If you're doing

File name: Compliancy_Feb._28_FINAL.mp4

direct mail marketing, you want to make sure that whoever you're using to send those mailers, you have a BAA with, but if you're just working with USPS directly, it's not a concern.

Moderator: Wonderful. Someone else asks, what is the difference between password protection versus encryption?

Liam: In many ways, it's the same thing. In order to encrypt your iPhone, you need to turn on password protection. That is in essence encryption. Now, there are much higher levels of encryption, and that's where you get into the things that get way more deeply technical, even than what I am familiar with, but essentially, you can think about this in layers. You have a laptop that you work on to treat your patients, you want to make sure that laptop is encrypted, and that can be as simple as creating a strong password that you are required to put in to open the laptop, but then, where is the patient data within that system?

If it's in your EMR, your EMR is encrypted, but you also should have a strong password to log into your EMR. That provides multiple layers before you can even get access to your patient's information through your laptop. For small practices, that is usually more than enough. Now, there are certain types of encryption that go above and beyond just password protection, which are still recommended because then, if there was a cyber predator that gained access to your system, it would encrypt your files for you. A lot of those things can actually be activated on your laptops and computers for free. That's always worth considering.

For things like cell phones and things like that, yes, it's activating a password. It can be one of the same.

Moderator: Another question asks, if we do not use patient names or identifying information in any emails, we have HIPAA-compliant Google Workspace. Do we need something like Paubox?

Liam: Can you say that one more time? I want to make sure I'm understanding.

Moderator: Sure. If we do not use patient names or any identifying information in emails, we need something like Paubox.

Liam: If you are emailing a patient directly, even their email is on the list of 18 identifiers that is considered PHI, so just their email in and of itself is considered to be PHI, and you want to keep that in mind. It depends on what you're, it's probably still very low risk, so up to you, whether or not you're comfortable with it is technically would not be HIPAA-compliant without encryption, but everybody has their own tolerance as far as risk is concerned. I can tell you formally to the letter of the law, it's probably not compliant, but it is a low risk transaction if there's no other sorts of identifying data that's there.

Moderator: Wonderful.

Liam: No treatment-related information, all that stuff.

Moderator: We have another question asking, how important is HIPAA-compliance in cases where candidates or employees are assessed for purposes of recruitment and selection, personnel and group development or talent management?

Liam: It's always a good idea to do background checks on the people that you're hiring. That's not usually expensive. You could do background checks for \$30 a person. There's a bunch of services that offer those sorts of things. One of the reasons why that's a good idea is there is something called exclusion checks in healthcare. Meaning that if somebody was previously convicted of fraud, they actually get put onto a list. The Office of Inspector General and healthcare organizations are required to compare their employees to that exclusion list. You can accomplish that with a simple background check. Y

ou can legitimately also just Google OIG exclusion list and just look up the employee's name. If they've been convicted of fraud, waste or abuse in the past, they'll pop up in there and then that that's somebody that you shouldn't hire. That's a very simple way that you can be more compliant in the hiring process, but otherwise it's really a function of post hire, training that person, making sure that they read and agree and sign off on your policies, things like that.

Moderator: Someone else asks, when buying a new computer, what's the safest way to transfer all necessary information? Is there someone I can hire?

Liam: That could be a good thing to get outside help for. Yes, so either an outside service or outside help to help you transfer all of that data. Transparently, having all of that information stored locally on a laptop is generally a bad idea. It's much better to have information in a secure cloud environment. We talked about Google Workspace before. Rather than storing your patient information on your laptop, which can be much more easily compromised, it's way better to have it in something like a compliant Google Drive or even a compliant Dropbox environment. All of those can be encrypted. They'll sign business associate agreements with you, and then that you have secure document storage.

Microsoft has a very similar feature. Also, if you're using a practice management software, an EMR, an EHR, those are also great data storage options.

Moderator: Someone else asks, what about Apple iCloud and Google Drive for business information?

Liam: Apple iCloud is not. Apple products, iMessage, iCloud, all of it, not compliant. You shouldn't be storing things like on an iPhone, generally speaking. If you have like access to your portal through an app on your iPhone, that's totally fine, but stored on the phone itself really shouldn't be happening. Even things like FaceTime, not compliant for dental health purposes. There were certain allowances given for that during the pandemic, but those have since lapsed. Google Drive, Dropbox, Microsoft, all of those could be compliant and they will sign business associate agreements with you. Apple will not.

Moderator: We have time for about two more questions. One of them is, what is the name of the exclusion list when you are looking to hire someone new?

File name: Compliancy_Feb._28_FINAL.mp4

Liam: Yes, so go on Google and legitimately Google OIG exclusion list. You'll get access to a massive spreadsheet and you'll be able to search a database in there where you can actually find out if somebody is on that list.

Moderator: We have someone else ask, how should a therapist obtain consent for a patient who uses Zelle or Venmo if the provider does not bill insurance?

Liam: There's something called an electronic communications consent form. That is probably similar to what you might want to have for something such as this. In that sort of a case, you're not billing insurance. It's not as much of an issue as far as compliance with HIPAA is concerned, but it's also not a bad idea just to legitimately make your own form that the patient signs stating that they are comfortable submitting payment through non-HIPAA compliant platforms like Zelle or Venmo, if that is their preferred option. That could be just something that you make for yourself. It doesn't have to be complicated with a ton of legalese. It's just getting the patient's consent that they're okay with this.

Moderator: I think we have time for one more question. Can you talk more about secure portals or platforms for email, i.e. Proton Mail?

Liam: Yes, so secure platforms or portals for email. I like to think of this in two ways. The actual security of the patient's information, but then also ease of use. One of the things I personally find it very difficult to use a lot of the more common email encryption platforms, Proton Mail, and maybe even Hushmail being two of those because it's not user-friendly at all for the patient. Your patients have to log into a portal every time they get an email from you. They can't just open up the email and read it if they choose to, especially for small practices where you're not communicating a ton of high-risk data, it is a little bit of overkill.

That's why I do recommend solutions like Paubox. There's another company called LuxSci, L-U-X-S-C-I, if you're looking for another alternative that is also a great fit for small practices. Those are great tools that can accomplish the same thing, but the email encryption is seamless, very, very easy for the patients to use. They don't even think about it. It's just encrypted automatically.

Moderator: We might have time to squeeze in one more question. What is the best way to get regular cybersecurity training?

Liam: There's tons of cybersecurity trainings that you could actually just purchase online. You're going to want to make sure that it's healthcare specific. Even you can Google healthcare, mental health, cybersecurity, healthcare, mental health, cybersecurity training. You'll see a bunch of options come up there. That is something that we provide as well through our platform, if you would be interested in something like that, but there's a ton of really, really cheap, affordable options that are out there for it as well. I can't think of any specific off the top of my head, but it would not be difficult to find by any means.

[pause 00:56:57]

Moderator: Maybe we have time for just one more. Thank you so much, Liam.

File name: Compliancy_Feb._28_FINAL.mp4

Liam: Yes.

Moderator: Can you direct clinicians to the protection of psychotherapy notes under the Privacy Act? Where can I find that information?

Liam: Let me see if I can very quickly find the specific CFR for that. If you want to look this up, it's 45 CFR 164.501. If so, if you Google psychotherapy notes privacy requirements, you'll see the definitions outlined within the federal codes themselves. We have some really free articles on this topic, so if you go to compliancegroup.com and you look up our blog, you can also just search therapy notes in there. We have articles that are written all about this topic if you'd like to check some of those out. That's all completely free on our website.

Moderator: That was our last question. Thank you so much.

Liam: Awesome. [crosstalk] Thank you all for having me so much. Really appreciate it.

Moderator: Thank you to all of our listeners for your participation. We'd also like to thank Compliance Group for making this webinar possible. A recording of this presentation will be emailed to everyone in two weeks time. The recording will include the presentation slides. As soon as the webinar has ended, a short survey will appear on your screen. Please take the survey and give us your feedback. We thank you for your attention and hope you have a great day.

[00:59:02] [END OF AUDIO]