MedPB CONNECTING PATIENTS TO PRACTICES

MedPB.com
888-469-5497
grow@medpb.com

Adapt to Thrive Transcript

Speaker: Josiah Dykstra

Interviewed by - Christina P.

Announcer:

Today, as part of our Adapt to Thrive web event, MedPB is proud to welcome Josiah Dykstra to talk to us about how practices can defend themselves. We don't like to brag, but when we looked for a cybersecurity expert, we looked for somebody the government uses to protect our national security. No joke. I'll tell you more, but it's all on a need-to-know basis. I could read you this long list of credentials, including a presidential award, but I think it's more relevant to tell you that he's the husband of a private practice owner. He also has a soft spot for audiology and has therefore been consulting with audiology practices for the last 15 years to help make them more secure. He's here today to give insider tips on making sure your practice is secure. Welcome Josiah.

Christina:

Welcome back MedPB's Adapt to Thrive, where we bring you the information you need to adapt to changes in the marketplace. I'm sure you've seen it in the news, cyber attacks have risen dramatically in the last few years, but you may not be aware that attacks on healthcare have been particularly brutal. MedPB's Adapt to Thrive is thrilled to have Josiah Dykstra with us today to talk about how we can protect ourselves. Josiah, I was reading that last year, four out of five healthcare practices have been a victim to some kind of cyber attack. That's an incredible statistic. Practices know that they have to be compliant with HIPAA, but what does that really mean now?

Josiah Dykstra:

First, thanks for having me. It's great to be here to talk about this. Cybersecurity can feel like a really big, broad, hard to get our arms around topic, so I'm glad to be able to talk to you about that today. HIPAA is a requirement. It is a law. It is something that every healthcare practice has to be compliant with. It's also the bare minimum. There's a lot that I talk about in cybersecurity in my business and with my clients, of things actually above and beyond HIPAA. The bare minimum for protecting health information is because some people wouldn't do any if they didn't have this compliance regime. So it's great that we have it, and we need to protect our businesses from the legal consequences of not following the law, and our responsibility to protect patient health information. That's an important goal.

Josiah Dykstra:

Cyber security isn't there to get in your way. It's to make sure that health providers can do the job that they love to do, that they're trained and qualified to do, which is provide healthcare and do it in a secure, protected mechanism. I would say the thing that people need to think about first is what is their risk? I can't tell you what is the top risk for your practice without knowing more about out an individual's practice. We hear a lot about ransomware in the press, for example, that might be a great threat to you, and it might actually be pretty low on the list of threats for any individual practice, but we all need to be prepared for the things that are the most common, things like phishing and the possibilities of data breaches, because those can have a real, tremendous impact on a practice.

Christina:

Right. What would you say is the biggest threat then?

Josiah Dykstra:

I think the biggest threat is not understanding the risk. Where are the strengths and weaknesses? Where are the things that any practice can play to? The things they already have in place, like policies and procedures, and to highlight the things that would help bring them into compliance or bring them into better security. If you didn't know that you needed to have your devices encrypted, that's a pretty important one. On a risk assessment that I do with a client, I would put that very much at the top of the list. We can never get cyber risk entirely eliminated, just like we can't get rid of our risks in our cars, or our homes, and that's why we buy insurance, and we wear our seat belts, and we put in fire extinguishers, to help minimize risk if something does go wrong. That's what cybersecurity is there for. I can't make your cyber risk go away, but I can tell you the places that you are accepting the most risk that you might not have even known about.

Christina:

Yeah. Some of these attacks, they can cause operational interruptions also. Some of them, I read a third of the attacks resulted in practices closing for seven hours or more. Why might that happen?

Josiah Dykstra:

Cyber incidents can be very disruptive. We all have a lot of digital data in healthcare these days. That's a great thing. It makes healthcare more efficient. It means that health providers can share more easily. The healthcare outcomes have been proven to be better because of this digital information. That is also a risk. If we can't get to our electronic systems, if we can't get into our building because of a pandemic, or a fire, or anything else, without having prepared a plan for what to do in those scenarios, it can be very disruptive. Not that it isn't disruptive no matter what, but having those plans are sometimes required by the law, HIPAA does require a contingency plan, but it also helps protect the business and make sure that no matter what happens, you can do the things that you need to do.

Josiah Dykstra:

Now, cybersecurity for healthcare is actually unique among cybersecurity for other domains, like banks, or even our personal information. The government says that we have to assume data breaches if anything bad happens on the network. The reason that they made this rule is, quite frankly, to make sure that health information is as protected as possible. If your antivirus scanner goes off, the government would say in the event of an audit, you should assume a data breach from anything like that unless you can prove that protected health information is not at risk and you have adequately protected it. All of the other components of HIPAA, things like backup plans, and encryption, and training, all of those minimize the possibility that just because your antivirus scanner went off, that anything was compromised. You can get around any potential fines or audits by showing, "Yes. Look, I was doing everything correctly."

Christina:

All right. If you were to prioritize what practices should focus on, where would you go with that?

Josiah Dykstra:

Certainly that risk assessment is the way to get started. Most often the thing that I tell people is, start with policies and procedures. Having those in place is a relatively easy, cheap thing that can be done. Some people have employee manuals, or security policy manuals, that are a good start to this, but to make sure they're up to date, they're comprehensive, and that they check all of the HIPAA compliance check boxes. For example, many people in their employee manual probably should add a password policy. The password policy would say the minimum length of your password should be however many characters. You're not allowed to share your password or to give your password away. That is just a cover your butt kind of business choice that many people should make. If you don't have that policy and somebody just gives their password to their colleague, or it gets out on the internet, you have no recourse as a business owner. If you didn't prohibit it, it was allowed. You need to write down that that is not okay. That is not allowed, in the same way that you should have a social media policy. What are people allowed to do on social media, or say about your clinic on social media? As a business owner, you should have a firm grasp on what is allowed and not allowed.

Christina:

Wow. I know that's a lot to keep up on also. I mean, things seem to change constantly. I know that there are some best practices you can do on keeping your software up to date, doing any automated updates, keeping your virus software up to date and all of that, but I also think it's a really good reason to invest in some additional help in terms of security, because these things are changing all the time. Last year, I know during the holidays, there were quite a few attacks because they knew that people had their guard down and they were off. To be HIPAA compliant, you need that certain level of security and you need to have things documented. Can you lay out some of the things that they need to have in place to be compliant?

Josiah Dykstra:

Yeah, it's quite a long list. When I do risk assessments with people, we walk through this sort of, the breadth of the law, because there are a lot of things that are either required or mitigations that can be in place. It does start with naming, for example, a security officer. There must be a person in every practice who has the formal role, it's often the business owner, that they are the ultimate person responsible, and the rest of the workforce knows if I see something suspicious, that's the person I need to tell. The identification of a security officer is a requirement. Many people have never sort of written this down on paper, but the more documentation you have the better. If anything ever goes wrong and the government wants to understand what happened in an incident, they will want to know, show me the documentation that everybody knew who the security officer was. That's a really easy first and foremost kind of thing.

Josiah Dykstra:

Then there's a whole bunch of policies. You must have, for example, an incident response policy. Some practices have this, and some don't. I can create these. Some of the professional organizations can sell you a template. The incident response plan is not just for a data breach, but it is a documented procedure about if the computers aren't working right, what do we do? What is the name and the phone number of our IT security company? Or maybe your attorney, or your insurance agent? That is a document, a piece of paper, that everybody in the practice sort of understands, here's what we're going to do.

Josiah Dykstra:

We talked earlier about a contingency plan, which documents, again, documentation important, how are we going to back up our data? Having that written down is a good first step. Eventually, you will need to implement that plan, which is let's make sure that the technical software is configured to do those backups. Then we have to test the plans. Just having a plan on the shelf that doesn't work is not helpful to anybody. It's great to have that plan, but making sure that the data is actually backed up, and furthermore, that you can restore. Actually go home and try and access your Carbonite backup, or your Google Drive backup, to make sure the data is up to date, that the systems are working. Those kind of routine tests are really helpful.

Josiah Dykstra:

There are lots of these other requirements. The other one that I'll mention is something called a Sanctions policy, which is like the password policy I mentioned. If employees don't follow the rules, what are the consequences? HIPAA requires this to help hold the workforce accountable. You get to define this. HIPAA doesn't say, "Here's what the punishment might be for this kind of offense." But every business owner should think about, what is the consequence if my employees access financial data for the clinic that I don't want to? What happens the first time? What happens the second time? These can include everything up to termination. If you have an employee who is stealing your money and healthcare records, that should be a fireable offense, and it must be written down and documented. Some of these feel like business decisions, and they are, but they also have impact to electronic health information, which is why they line up with HIPAA.

Christina:

Is it always the owner that is the privacy officer and is responsible for all of that?

Josiah Dykstra:

Often it is the owner in a small private practice. In a hospital, this wouldn't make sense. In a large, sort of distributed enterprise, it doesn't have to be the owner. If a clinic has 10 locations and a substantial staff, the owner could delegate that responsibility to anybody in the practice. It does not have to be the owner.

Christina:

Right. There's plenty of checklists for these types of things, but I think going through them and making sure that your plan stands up to scrutiny is crucial, I think, for a lot of people. Practices are also required to do regular training with their staff and to make sure they're keeping up with the latest information. What kind of training do they need to do? How frequently do they need to do that?

Josiah Dykstra:

HIPAA does say you must do training. It doesn't stipulate the kind, or the frequency of it. Although, most professionals interpret HIPAA as having a yearly requirement for all staff. It says that the training must be current and updated. It says that it must be appropriate to help people do the jobs that they have in the practice. You can probably find free HIPAA training on the internet, but I will say you get what you pay for. It probably is not as updated and not as applicable to a particular clinic, as customized training might be. A once a year online training probably makes you compliant, but not very secure. You can certainly have both. You can be both compliant and insecure.

Josiah Dykstra:

I recommend building a more comprehensive culture of security. Talk about security all the time. Don't make it a negative punishment kind of thing for employees. Make it fun. Make sure they know they won't be punished by turning in, reporting suspicious activity. That can all be part of that routine training. One thing I do for some clients is monthly emails. I send them just a security tip, like, "Hey, just so you remember, when you go on vacation, don't put that on social media." That can actually help protect patient information and the business, but just reminding people on a routine basis, more than once a year, more than what people say is required, does build a really productive culture of security.

Christina:

There are certain events that should trigger them to do some additional training. For example, if you're opening a new office and you have new employees, or if you think there's been some kind of breach, is there a service or a setting that could prompt them to do regular updates?

Josiah Dykstra:

Yes. Let me answer both questions. First, about triggers. There's lots of things that might lead you to think that something just isn't right. Lots of people just have a gut instinct. My computer is slower than it has ever been before. Something has changed. It might not be that we got hacked. It might just be my software is misconfigured, or there's an update installing or something, but that is a reasonable trigger to go look and see what happened. In the very extreme case, you might get a call from the police, law enforcement, the FBI, that says, "We found your health information, your practice's health information, on the dark web, on the internet." That's a really bad day, but some people do learn about data breaches in that kind of way.

Josiah Dykstra:

HIPAA also says that you should regularly review the audit logs. If you don't know how to do that, these are settings in your computer that can say, every time somebody logs into the computer, write down in the little file, on the computer, automatically, who logged in at what time. That is great information to troubleshoot things that are going on. Looking at those logs, things will pop out to you. Why was that employee logging in in the middle of the night, or when they were on vacation? All of those can help uncover things that just might be going wrong. Those regular audit reviews, and having a professional look at your systems, too. We all go to the doctor, not because we're afraid usually of what the doctor might say, but because we want to be healthy. Hiring a cybersecurity company to do an evaluation, to do an assessment of the cybersecurity, they can also look in the nooks and crannies of the computer and tell you, "It looks like something might have been going on. I will help you understand that." All of those are good triggers.

Christina:

Right. I go to the doctor once a year. I go to the dentist several times a year. How frequently should people look into security?

Josiah Dykstra:

Honestly, it should be a continuous thing. It doesn't have to be eight hours of your day, every day. That's more burden than it's probably worth for you. But to take some time, once a month, to just remind employees, do your annual risk assessment, those are all really good kinds of things. Even if you're doing all of the right things, stuff still goes wrong. I have started to recommend that people look into cyber insurance as a backup for the unexpected, catastrophic kinds of events. I have auto insurance and homeowner's insurance that I hope I never have to use, but the auto insurance industry knows that people get in car accidents. That's one reason that is required in most states. Cyber insurance can also help lower your risk from catastrophic events that were just beyond your control. This is not a HIPAA requirement. HIPAA doesn't say anything about insurance, but I think as a business decision, it is an economical way to manage risk.

Christina:

All right. To wrap up, what are the seven things that practices can do today?

Josiah Dykstra:

Absolutely. Number one, do a risk assessment. Understand where your risk is today, where you didn't even know you had risk, or where you're accepting risk that you don't want to. Do that first and foremost. Number two, do that HIPAA required incident response plan. Find a template or hire somebody to help you make sure that that is current and updated and actionable before you even need to use it. Having that before an incident is the most valuable to you. Number three is similarly to develop a contingency plan. Review the one you already have. Update it or create one if you don't. Get yourself into more HIPAA compliance and protect your business with that contingency plan. Number four, review your Business Associate Agreements. These are required by HIPAA, and for anybody who handles your protected health information, whether that is an online service provider, an email provider, even your cleaning crew. If your cleaning crew walks in in the middle of the day, sees the patient in the waiting room, or can see the screens, they are exposed to protected health information, and you should ask them to sign a BAA. Make sure those are complete and up to date.

Josiah Dykstra:

Number five, I would say, is review your security culture. Think about the current training that you have. Does it need to be more routine? Does it need to be updated? How can you give positive reinforcement to the workforce? Or think about some creative ways to test security, maybe think about a fake phishing campaign and how might they respond to that? Make a game out of it. That's number five. Number six is be very careful about anything that stores or touches protected health information. In particular, when your computers are replaced, when you get rid of an old computer, make sure that those hard drives are properly sanitized of all of that information so that even a security expert can't get it. Just the way that we protect papers with shredders, make sure everything that touches digital health information is clean. Number seven, think about cyber insurance. Talk to your current insurance provider, see if maybe you have it and didn't know it, or if that current provider can offer it to you. If you need to look at others, the big companies on the market, like Chubb and Farmers, all of them offer cyber insurance policies, see if that is right for you. So, those are the seven that I would say to prioritize.

Christina:

That's great. If this all sounds like Greek and they don't speak Greek, what should they do? What resources are available for them?

Josiah Dykstra:

Stay calm. It can be overwhelming, but you can do it. There's lots of things within your control as an individual and a business owner that you can do. I have done research about audiology practices and it shows a huge range of talent and compliance. I'm happy to send you that research so you can see that there is some breadth here. We all, as professionals, as medical professionals, need to raise the bar and be as secure as we can. Talk to your professional organizations. AAA, ADA, offers resources to people. I know ADA sells a HIPAA bundle, which I have looked at and I endorse. Make security a priority. Just because it seems like Greek doesn't mean you shouldn't do it. Maybe all the more reason to hire somebody to help you out. Set it as a goal for the last two months of the year, or for the year 2022.

Christina:

Great. How can they contact you if they have questions, or if they want a copy of that, the trends and cybersecurity behavior, and more additional information?

Josiah Dykstra:

Yes, the easiest way is by email. You can email info@DesignerSecurity.com. That email address is also on my website designersecurity.com. I'm happy to send you that research. I can also send a presentation that I did on how to secure smartphones, "Seven Steps to Safer Smartphones" with video tutorials on how to do that for Android and iPhone.

Christina:

Well, and that's crucial, since a lot of practices had to close for COVID and started using their cell phones when they're not always as secure as people think they are. That's fantastic! I want to thank you again for joining us today, and have a great day.

Josiah Dykstra:

Thank you very much. Bye bye.