Therapy Tech With Rob and Roy:
How To HIPAA-fy Your Practice Tech in 2014

Roy: Broadcast is live. Hi everybody. This is Roy Huggins and we’re having quite an interesting morning over here at Therapy Tech with Rob and Roy Central. There’s probably quite a few of you who are watching right now and we're still trying to get an email out to you to tell you the right link to click. It might take several minutes for that email to actually get out to you, but you guys will join us. My apologies for the very slow start this morning.

What's happening is Google once again as they're prone to do, has changed all of the interfaces for everything that you do with Google Hangouts on air and everything we expected about how it will work, is completely different and nothing worked. We had to take all this time to try to get it all working and then of course there's all the overhead of trying to make sure we get the message out to all of you about the new place to go. This has been good times. Yeah. Right. It's been good times, but I ...

Rob: Everybody send Roy a warm fuzzy e-mail later today.

Roy: Please. I’ve been getting lots of email to say, “Where are you?” I'm like I'm trying. I'm trying to fix it while you're asking. Okay. Hi Rob. How are you doing this morning?

Rob: I’m doing well, Roy. What about you? Now that you are through the more acts and drinking your coffee?

Roy: You’re right. I'm fabulous. It's so good to be here. Okay. This episode is going to be a shorter one because we've got to go at 11 but we'll do our very best to get all the good information out to you. Luckily this is not a continuing education event. This is a show. If you're not familiar with our show, you should be aware that it's a very irreverent show, where we definitely are going to give you serious information but we're not going to be super serious about it and we actually have a special guest today.

Let me make sure you know who Rob and I are real quick. I am Roy Huggins. I am a former techie, now I'm a professional counselor in Portland Oregon and I have various qualifications like I'm the technology chair for the Oregon Counseling Association. I joined the faculty of Portland State University’ counseling program. Other than that, Rob tell us about yourself.

Rob: I’m Rob Reinhardt. I'm a licensed professional counselor, supervisor in North Carolina. I also run my private practice as consultant with a focus on technology and I write a column for the Counseling Today magazine and I also focus on technology.

Roy: Right on. We have a special guests here with us today. You guys are surprised. Now he's having some technical trouble. His computer insists that he doesn't have a camera which is not true. His name is Clinton Campbell. Clinton why don’t you say hi for us.

Clinton: Hey, Roy, how is it going? Hey guys. Thanks for coming.
Roy: Going well.

Rob: Nice to see you Clinton.

Roy: Clinton has a pretty good bio which I can't read to you for various reasons that I'm going to blame Google for right now but what I do know is, so Clinton possesses 2 masters degrees. He is a professional counselor in Seattle and he has a master's of counseling just like Rob and I, but his history behind that is very interesting. Clinton also has a master's degree in, it's not in Computer Science, right? It's Information Technology?

Clinton: Its computer science with a specialty in security.

Roy: It is computer science. Right. Clinton actually has a master's degree in Information System Security which geeky people like to call Info Sec for a shorter name right? That is correct. That is your masters right?

Clinton: Yes.

Roy: Right. Here's the cool thing and I know Rob will probably jump in on this one, is that for 4 years after getting his master's degree, Clinton actually worked for the NSA and I know that's one of our favorite organizations here on Therapy Tech with Rob and Roy. My question for you Clinton is when you worked in the NSA, did you spy on my e-mails?

Clinton: I could tell you but I'd have to kill you.

Roy: Oh, okay. Right on, thank you. Right. Okay. Of course in our second show on EHR systems we talked quite a bit about the NSA and the recent news about NSA spying on e-mails and such, so we might make fun of you but not as much today because we have half the time that we thought we did. Yes. Clinton's back on.

The reason I have Clinton on today, is because while we're talking about HIPAA compliance with technology, we're primarily talking about the HIPAA security rule. The HIPAA security rule was designed by security professionals really. Basically it's just taking good practices from the security world, made a few quirks for the healthcare industry and put it into law.

With Clinton's background, his understanding of where the HIPAA dictator rule comes from, is really deep and it's highly professional. As in fact Clinton doesn't just have a master's degree, he also has a particular professional certification called the CISSP. Do you want to tell us really briefly when that certification is Clinton?

Clinton: It's in a nutshell its Certified Information System Security Professional and it's pretty much the general baseline for security professionals that have reached a certain place that have a core set of expertise in all of the different parts of information security. They can talk well about risk management, they can talk well about network security, and they can deal with crypto, at least on basic level.
The CISSP is a professional service. It's trying to establish kind of a baseline for who you're working with there.

Roy: Right. Great. In my experience when I've been studying HIPPA, I have noticed that in doing hospital systems, also at the state level, when the people who hold the positions of being HIPPA security officers or compliance officers, many of those people hold that CISSP certification. Is that your experience Clinton?

Clinton: That is and within certain groups, businesses, within the government, you’re required to have that. The whole physician at a certain level.

Roy: Right. Right. You’re required to have that. The reason I brought Clinton today is because he holds that certification and he is also a professional counselor. He holds that license as well and so he’s got that unique mix that Rob and I tend to have except that Clinton doesn’t publish as much as we do. That's the main difference. First Clinton’s background is much, much deeper.

I know we’ve got some questions from people and so there's a couple of question types I want to address. One is a number of people asked online therapy software and we in our first episode of the show, we talked about that. You want to go back to our YouTube channel and the first episode of the show it’s all about online therapy software so check that out. It’s really great. Also a couple people asked about forms and that's part of the HIPPA privacy rule.

I often forget that the HIPPA privacy rule is there when I'm talking about training so I apologize for that. In the resources so when you get the e-mail, there's a resource links and also on the web page, there's resource links. One of the links is a link to some models of the new notice of privacy practices .after September 23rd, 2013, you do need a new HIPPA form, which is often called Notice and Privacy Practices.

In there, there's a link and the feds have given you a model that you can use to make your new Notice and Privacy Practices so click that link and its right there. It’s really handy. It’s free. Otherwise we're going to talk to have to talk about ...today we’re going to be talking about the bigger subjects of the process of HIPAA compliance. Specifically, the beginning of it, which is risk analysis and risk management planning.

That’s probably why Clinton is here because that's his big expertise and I also do that as well. Rob, do you have any comments about that? About HIPAA security?

Rob: I do. I just want to point out there are a lot of specific questions that were submitted to us before the show, that we probably won't get to answer a lot of very specific questions about how do I make sure I can use my mobile phone securely in this, that and the other, but the information we’re going to cover is a very big, is an umbrella starting point for assessing any situation using technology.

Of course, if you have detailed questions you can certainly contacting one of us for a
consultation about how to apply what we're talking about today to specific situations.

Roy: Of course that's why we write. That's why Rob and I write all these articles is because there are so many specifics that can't be covered in something like this because it's specific to one or a small group of people. For example, a number of people ask about iPhones and iPads. I have a pretty long article about how to secure iPhones and iPads. Go look for that on my website and you'll see it there. Rob also has a number of articles about electronic health record systems.

When you're looking for those specific tech details, you look for our articles because that's actually usually an easier way to get that information and make sure that you get the specific information you need. Of course we haven't covered every single subject, but we've gotten pretty far at this point. We've covered quite a few. Right. Let's get started and let's just talk about how do you do HIPPA compliance.

Rob, Clinton jump in here if you feel I'm missing anything, but I'll tell you that the way HIPAA compliance works, what the HIPAA security rule requires you to do, is to start off with what's called a risk analysis. I know I have my definitions of that, but I'm going to let Clinton talk about it because he probably can talk about it much more academically than I can, but first I want to ask Rob, like Rob, what's been your experience when you do a consultation with people about how they use risk analysis or how you deal with that with them?

Rob: A lot of people don't even have a full on understanding of what that is, so it starts with educating about what the process is and that's another thing that I have an article about that bullet points, the steps of going through it. First to understand it, I usually employ analogy. People have this understanding or this false understanding that, as long as I use a bunch of compliant pieces, compliant software and compliant this then I'm good, but that's not the case. There's a lot more to compliance. This risk assessment is that they piece of it.

Roy: Did we lose Rob? We lost Rob. Okay.

Clinton: I think we lost Rob.

Rob: You lost him.

Clinton: He’s just back.

Roy: You're back with us here Rob.

Rob: I didn’t go anywhere. The analogy I use to help people understand risk and risk analysis is that, we take risks every day. Every time we get behind the wheel of a car we're taking a risk. You're risking everything ... Then risk analysis is about going down the list of things that could happen. You could have mechanical failure or blow a tire or the engine, the transmission drops out. You could run into dangerous drivers on the road. People talking on their cell phones or driving under the influence.
You could have inclement weather. Whether it's sleet or snow or rain. It's a matter of going down this list of things that could happen and doing everything you can to mitigate those risks. You can't ever have a situation where there's absolutely no risk. That's where people get that idea of, as long as I use everything that's compliant, I'm totally covered. No, they're still risks and you have got to document those risks and what you're doing to minimize them.

Roy: That's the key, right? You've got to document the risks?

Rob: Right.

Roy: Is there anything in our old profession that you don't have to document? I can't think of what that would possibly be, right?

Rob: No, no.

Roy: No, yeah I can't. I really can't. I was actually trying to make stuff up. I really was and I can't think of anything that you're not supposed to document.

Rob: Tiring form consent documents. They're like 8 pages long.

Roy: Right. I think yeah. Mine's almost there, that's true. Especially with the notice of privacy practice, the HIPAA form, right? That's the risk analysis. That's a great analogy. The whole idea is that the practice has risk in it too. With the HIPAA security role, they want you to think about those risks when it comes especially to technology. They want your electronic protected health information to be covered.

They want you to look at all the risks to it and they want documentation that you did that. That you took a look at all that. What's interesting is, a lot of people will come to my trainings and I'll talk to them mostly about how to mitigate the risks. Like here's how we do stuff with phones. Here's how we do stuff with computers. Here's the problems with email. Here's the problem with texting. Here's what they do about it, because that's the nitty-gritty info people need.

Then what I've noticed that people don't always come away with and I need to figure out how to do this better. This is obviously me not expressing it well is that, they need to document that they looked that what the potential problems are before they solve the problems. That's the risk analysis piece and that's actually a key part of HIPAA compliance. I'll tell you the head of the Office of Civil Rights, which is the federal office that enforces HIPAA has said that, going into this year, they're going to be emphasizing risk analysis.

If they end up auditing an entity and I'll tell you, the likelihood that they're not going to randomly audit us, us solo practitioners, a small group mental health, they're not going to randomly audit us. That's not going to happen. You'll probably get audited if you have a complaint or you have a security breach that you have to report. That's probably the
only times you’ll get audit, but if you were, they’re saying, they’re emphasizing they want to see that the entity, that the clinician has done a risk analysis, they’re going to want to look for that.

I’m going to ask Clinton. Clinton, we had talked a little bit about this in an analogous way. Why don’t you tell us a little more detail, a little more academically what a risk analysis is. I’d love to hear, I know you have some wonderful philosophical thoughts about it too, so tell us about that?

Clinton: Let’s see where to start. First thing I would say, is that a risk analysis, you talked a lot about managing the risks and mitigating some of those risks. The risk analysis, the reason it's part of HIPAA is that it fits into the concept of risk management. The idea is that, within our practices, within our business processes, we have all of these risks as Roy and Robert talked about.

We’re going to have them as soon as we start to use email or as soon as we start to text or as soon as we start to have clients that are going to find our emails and send us messages that contain personal information. We very quickly start to build up risks and it’s easy to think about them as small and nonexistent because we’re not driving down the highway with a lot of other cars around us. We can’t see the other cars passing by. We can’t see the hackers buzzing by us on the inter-webs.

Roy: May be you can.

Clinton: In general, the average person isn’t going to notice those things on a day to day, so they’re not thinking, they’re not mindful of what all is happening while they’re working with information and while they’re working with technology. The purpose of the risk analysis is to get your mind around that. To work with somebody, to work in a systematic way to break down what are the different parts of my system?

What are the different types of threats that are out there? Which has a lot to do with who’s your clientele and who are you and what type of technology do you use? Then what sort of vulnerabilities are known by professionals in the field? If you take those different pieces, the vulnerabilities, the threats, the different parts of your system and you put those together you can start to assess, “Okay, where are the areas that I need to improve?”

Where are the areas that I might not have thought about well enough so far?” Then I think with HIPAA and this is a direction a lot of compliance frameworks are going is that, they’re not starting from a point you check off A, B, C, D, E, F, G. They’re starting from a point of, we have ... We have this documentation that you have to have in place as Roy and Robert mentioned. You have to have a risk analysis. You have to have a policy. You have to have a business associate agreement.

You have to have those things in place, but when it comes to vulnerabilities, what we want to see is that you know what they are. You know where you stand in terms of risk and that you’re working diligently to fixing those things. You’re not going to be able to
look and take your system, especially if you’re an established practitioner and you’ve been doing things a certain way for a long time. There might be things that you need to fix right away, but you’re not going to be able to take that system and fix everything on day one or year one. The idea is that you’re going to continue to improve and that’s evolutionary.

Roy: I don’t have to do my risk analysis, find all my problems and then fix every single one of them tomorrow or Tuesday. I don’t have to do that?

Rob: You have until Thursday I hear.

Clinton: You have until Thursday. Yeah.

Roy: Thanks Rob.

Clinton: It’s a misnomer that you could [Crosstalk 00:17:08].

Roy: I was joking everyone by the way. I just want to make sure you know that. Sorry Clinton, go ahead.

Clinton: Oh, that’s all right. I was going to say that’s a misnomer to even think that you could find all your problems. We were talking last night Roy, kind of just brainstorming some things for this session. I was saying that my goal with an initial risk assessment year one for somebody or let’s say the first 6 months would be to find the top 10 problems. First off, let’s iron out all the details. Let’s make sure you have business associates agreements and that you’re using HIPAA friendly services, HIPAA friendly cloud service providers, email, all of that as …

Roy: HIPAA friendly would usually be like, they would probably call themselves HIPAA compliance, but we know that that’s a misnomer when a product says I’m HIPAA compliant. Only the clinician can actually be HIPAA compliant, right?

Clinton: Yeah. We start from there and then we look and we say, “Okay, now, what else is left? What’s still hanging out there? What are the known problems?” We look in and say, “Where have you implemented encryption and does that actually cover all of the types of problems that you might have?” For most of you, if you don’t have a background in information security and if you don’t have a background or a solid understanding of at least the basics of encryption, it’s not going to be very easy for you to figure that out on your own.

You’re going to need to consult with people that whether it’s a friend, whether it’s somebody that has good tech experience and that’s also a little bit versed in compliance or whether it’s one of these guys or myself. You’re going to need to bring somebody in to look at that and to say, “Okay, where do I go next?” My goal would be … We’ve got the basics in place, now let’s look at the 10 biggest things that you have to do and that’s going to be the focus or maybe it’s 15, but it’s a manageable number that you’re going to handle and we get those going and move forward.
Roy: Wait, wait, wait. If I only do the top 10 or 15, then I haven’t covered everything, right? Then how am I HIPAA compliant? Don’t I have to have the right stuff in place to be HIPAA compliant?

Clinton: I think in this situation, compliance is a process. Compliance is showing that you’re actively engaged in the process and that you’re continuing to move forward in that process. You start with the 10 biggest things and you work actively on managing those risks and dealing with those. By the time you finish with those, you’re probably going to have identified some new things and you’re probably going to have another list of things that you need to tackle, but the reality is that, it doesn’t help you much as an individual to have 100 different items that you need to check off today or tomorrow.

We need to start with manageable chunks and we need to start in a way that keeps us actually engaged in the process rather than overwhelming me and having me say, just forget this, I’m going offline and I’m going back to paper files, I’m not [crosstalk 00:20:08].

Roy: Yeah. Rob and I … Sorry Rob go ahead, sorry.

Rob: I’ve got a 2 part question with that. One, what I’m hearing is ideally, once people decide, I’m entering into this process that would be a good idea to then not engage in any new technology unless you do that risk analysis, but also I’m curious to hear since a lot of our people watching this have really probably never done a risk analysis, they’ve never started down that road. What would be maybe the top 3 places you’d suggest that they start?

Clinton: That’s a good … That’s a good thought. I think one of the biggest things, one of the hardest things for most people to get their mind around is really clearly defining and the technical terms we say, it’s defining what your system is. This is where I got a little philosophical talking to Roy because I look at a system as including the people that are involved in it and I look at a system as in terms of a therapist and individual practitioner, your system is, let’s say your computer and your tablet and your mobile device and that’s the networks you connect on.

Your favorite coffee shop or the bar down the street or your office and your home network. That’s number one for me, is getting my mind around what are all the different pieces of your computing environment and trying to place some constraints on that that are reasonable. You made the point a second ago Rob that, once you start in this process, it’s a good idea to not bring anything new in right away without doing some risk assessment on that as you go and I think that’s absolutely true.

It might actually be a good idea for a lot of people to rule some things out. For example, you have a laptop that you use for your practice and your kids also do their homework on it. It’s going to be a lot easier for us to do a risk assessment and mitigate the risks if we can eliminate that issue. If we can …
Roy: It’s okay for my kid to do homework on the laptop that I use for my practice?

Clinton: Possibly, but if we do that, we’ve got to look at what extra risks are introduced.

Roy: The reason I’m asking is a lot of people will ask, the way they’ll frame it because this is the way it’s been put into our heads as clinicians is like, I’m going to have a X circumstance and then there’s some judgment that needs to be passed by an overarching body about whether that’s compliant, whether it’s acceptable. There was an idea of, someone wants to know, hey, is it HIPAA the compliant if my kid uses the same computer to do his or her homework?

What we’re saying is, it’s not about is it complaint or not. It’s an issue of, can you can you identify the risks of doing so and can you reduce those risks to a reasonable okay level, that’s what you’re saying, right?

Clinton: That’s what I’m saying and that’s in terms of my point about number one thing being defining and constraining what the environment is and what the system is. It’s exactly that, it’s if you can’t define and constrain the environment, you can’t identify all the risks. If you can't narrow it down to 10 or 15 big ones, you can’t narrow it down to 2 or 3 to start with, because you’re going to be overwhelmed and flooded with all of the possibilities.

Roy: How would you constrain it? You’re a solo counselor in private practice. You have an idea of what kind of systems people usually have, what kind of constraint would you usually say most of us would want to go with.

Clinton: I think some of the things that I have are one, simplifying. If you don't need 5 pieces of technology to manage your practice, rule a couple out. If you can do it with your phone and your computer, let’s stick with your phone and your computer. If you can keep your calendar on one device or another and not have to sync it through the cloud, let’s do that. If you can rule out working and this may be difficult for a lot of people, myself included. If you can rule out working on a coffee shop network, let’s do that.

Those are the simple constraints for me. The other types of constraints I would recommend with people and what I do for myself is that I stop looking at, it’s really easy especially when you get into the cloud services and the apps and all of that to get caught up in all the flashy new things that you can grab and become more efficient with. There’s a dozen new email providers that will intercept everything from your inbox and they’ll give you a really cool way of quickly categorizing and sorting through email and getting your inbox down to nothing.

Sounds very appealing to me, but at the same time, it's just not practical for me. It’s going to introduce so many risks and at the same time, it's going to introduce a new business associate who’s not going to want to be a business associate.

Roy: Right. We should explain what a business associate is because we don't want to assume that our viewers know all these terms. Okay. One, so business associates are like, when
Rob and I do this show I think we've had to bring that up ... Yeah, we've had to bring up every single time. We probably would never do a show where we don't bring it up. I always are the one who defines. Rob, do you want to define a business associate this time.

Rob: Is it my turn? Yes, so I think we do cover …

Roy: It's your turn, yes.

Rob: A business associate is essentially, if you're a covered entity, a business associate is anybody that you're sharing protected health information with in some form or fashion and they're basically signing an agreement that they will handle it appropriately. They themselves will take on the responsibility of maintaining compliance with HIPAA and they would have their own set of things that they have to do. Including a risk analysis and risk assessment and so forth.

Roy: They have to hire someone like Clinton to help them too, right?

Rob: Exactly.

Clinton: They also need to know ... I think part of the reason for a business associate agreement is this informed consent that you're actually letting them know that you're sharing protected health information with them.

Roy: Right.

Clinton: Which a lot of folks never think about.

Roy: Right. Definitely, we're faced ... We tend to face our clients. We don't face the businesses that we're working with and it's true. If you're putting protected health information in your Gmail account without Google knowing that you're doing that, you actually can get Google into trouble. Google can get into trouble for that and considering the trouble I've had this morning with Google, moving my half an hour of the show, I'm fine with that.

I'm going to give them protected health information, I don't care anymore. Sorry, wait. No, wait, wait, wait, wait. That's not good for my clients, sorry, okay. I won't do that. If it was just bad for Google, I would do it, but it's true. It's informed consent all the way around. As you're saying, the player is the people involved, there's also these services that you're using. We have a tendency to not think about the services we're using as a part of the clinical activity we're doing.

We tend to think of them as just tools like a file cabinet and that's not the worst thing. The companies that make these services market them and design them so we can do that. They want us to not have to think about it, but the problem is that, that for us clinicians who have to think about security and privacy, that creates our way of thinking about these services that tends not to help with that process.
We need to be thoughtful about how, hey, if we are using Gmail to talk to, not just clients, but also colleagues about clients, then that means Google is involved in that process and we need to think about how is Google involved and what HIPAA would require you do, is that you get a business associate contract with Google. Fortunately, Google happens to be one of the consumer level companies that will do that.

You don’t have to buy the business version or to get the paid version of Gmail, but if you do so, they will give you a business associate contract. You can actually ... You can bring Google into your risk analysis in a way that works for HIPAA compliance, right?

Clinton: Yeah.

Rob: I really like that Clinton talked about a system and I think that the way a lot of people in our field can connect with what we're talking about is if they’ve done family work or studied family systems therapy and think about how you’re not going to be working with part of the family and then bring out other parts of the family without thinking about what that process is for. What is your goal, what are the risks? We are talking about the same sort of thing here.

Clinton: Exactly. The thing I would point out here and this is something that I think it was the first time when I was in school somebody said, computer security and now counseling, those are 2 really different fields. I sat and I thought about it for a while and all of a sudden I realized, these 2 fields have the same vocabulary. When I was at NSA, when I was talking to folks there, we were always talking about boundaries and trust and vulnerability and it's all about communication.

It's all about sharing information between one another, getting it to where it needs to be and having some ability to ... It’s really, we're trying to externalize our mindfulness about what we will do and won't do and what's appropriate and inappropriate, when we're dealing with computer security. Now most security and techies aren't really savvy on the human relationship side of systems as much. Of course, the 3 of us excluded.

Roy: Yeah, maybe not Rob, I don't know. He’s very stoic.

Clinton: Exactly. It's all about systems and it really is about those same concepts and it's about communicating well and being mindful about who all is in the room and who all is part of that communication, when Google is your service provider.

Roy: Right. Let me just make sure. We're talking philosophic and I'm loving this conversation and I’m sure it's very interesting, but I know people came here to learn how to be HIPAA compliant so is this HIPAA compliance? You’re talking philosophically about systems and relationships, that's not HIPAA compliance, that's philosophy and clinical stuff, there’s nothing to do with it, right?

Clinton: Again, we get down to that question of HIPAA compliance being about risk management, and being about having a framework and a system for managing your risk.
Compliance is a little bit of a misnomer even for therapists, because it indicates having arrived, in my mind. It’s like being mentally healthy as a client or being cured as a client. We want to be cured and we want to know when is this going to be over? When am I going to be done with this?

The truth of it is, is that you're not done with it because communication continues to become more complex and you continue to rely on technology more and more and it's integral in who you are and how you talk and how you share your life with people, and the same is true for your clients.

Roy: Right. Let's make sure we give people an idea of what the process of risk analysis typically would look like. It's important to know that it doesn't always look the same, because there isn't one way you’re supposed to do it, but there are certain guidelines for doing it well, and in the resources links that we sent out for this show, I believe the first one is a link to a document that the feds have put out that gives you some guidelines on how to do risk analysis and risk management planning in a small entity.

You can go download that, and you can read through that, get some colleagues together, even doing in a group is great, it’s a great way to do your risk analysis. Read through it, and see if you can understand and try to make sense of it. I know they do try to write it for the small provider, if you hire a consultant, like I do risk analysis with people. I know Clinton does risk analysis with people. Rob do you do risk analysis with people?

Rob: Absolutely.

Roy: Right, great. I figured as much, right. All of us do this. If you want our help, we’re here, we can do that. Our contact info is also in that resources list. You can also as Clinton was talking about, if you get somebody with that deep technical knowledge, or as long as they know the security side as well, you can also get ... You probably want to get them to help you if you don't feel like you can understand the IT, the information technology side of what you're doing.

Generally, when you’re doing a risk analysis, you're going to start by defining the scope of what you’re looking at. Clinton was talking about defining your system, that’s where you put it, that’s ... He has a much more nuanced way of thinking about it. The scope being like, this is what we're going to analyze, these are the parts of the practice we’ll analyze. What HIPAA requires you look at is any parts of your practice where you have electronic protected health information, where you create it, where you receive it, you maintain it, any of those things.

They only require you look at electronic health information. A lot of security experts would say, “You should probably also look at your paper, not just electronics.” I would also consider your file cabinet. Then what you’ll do is actually a creative brainstorming process. You look at all of your assets that you have. It could be your cabinet, it could be your computer, it could be your e-mail account and you start thinking about, “How do I use all these things? How do I interact with these things?”
As you're thinking, you're looking for the risks that pop up. You're looking at vulnerabilities that they have, you're looking at threats that can bring in those risks. Threats can be things like, people trying to spy on your information. Threats can be accidentally disclosing information to the wrong people. Threats can be a power outage that cuts off your internet connection, and thus cuts off access to your records system. Those are all the threats that can happen.

Then you evaluate all those risks. The document that I'm talking about says you can just evaluate all your risks as being low, medium or high. That's all you really have to do. You don't have to do some crazy system evaluating risk, just low, medium or high. As Clinton puts it, after you've vetted all these risks. A risk can be something like if my laptop, my laptop could be stolen and my laptop has records on it.

If that happens then all these records will be exposed to the thief, and so you say, “Okay, that's a high risk because my laptop doesn't have any security on it yet.” That's a higher risk. When you go ... When you're done with the risk analysis and you do the risk management plan. That's probably your highest risk, is your laptop being stolen, and so you're going to say, “Okay, I'm going to make a plan for making that risk go down.”

Your plan's probably going to involve putting encryption on your laptop, and putting a firewall on your laptop and things like that. That's the general idea, you do the risk analysis, then the risk management. I have found when I work with people, doing risk analysis, it's not uncommon for us to find some new way of as Clinton's saying, ruling out tech that you don't need, and consolidating your tech so that you are able to actually sometimes, sometimes people actually save money.

Usually people spend a little bit more, like $5, $10 more a month. If they go for an electronic health record system, it could be $50, $75 more a month depending, but often doing so, they end up making their practice more efficient. With the risk analysis, it's like Clinton saying. It's not just the security thing and the security things sits by itself. You're incorporating a look at security and technology into the entire way you practice.

I have found that people can often make their practice more efficient that way, especially by doing what Clinton’s saying about ruling out stuff you don’t need. What do you ... Rob, I'm curious your thoughts when you've done risk analysis with people.

Rob: I think you did a great summary of just the general approach, and again it just keeps coming back to that systems analogy. Once you get that scope defined, you know exactly what pieces of the puzzle you need to look at, all the rest seems to fall into place from here.

Roy: Yeah, that's true, and it is true that you often need a techie to help you find what some of those risks are because if you're not familiar with the end of the hood, I think it was Clinton that was saying, your analogy of you’re driving on the road and you know the other drivers are there and Clinton’s saying, you don’t see the hackers, you don’t see the bits flying by, so you definitely need a techie.
Rob: We talk about hackers and that seems to be the first thing when I talk to people. They go to, “Is my information safe? Who’s going to get access to it?” You’ve got to look at the big picture, what happens if you have a fire or other catastrophe. There’s a number of other things that could happen that have nothing to do with somebody trying to steal the information and those sorts of things. Again, just to reemphasize because I’m not sure if you totally emphasized in it, all this has to be documented.

Roy: Oh, right.

Clinton: What documentation?

Roy: How do I do that?

Roy: Do I write it down? I don’t understand. I am totally unfamiliar with the concept of documenting my work. This is not something I do.

Rob: That’s the thing people in our field, many of them anyway. That’s part of their job that isn’t their favorite is to even document client paperwork.

Roy: Oh yeah.

Rob: Then you talk about, oh, now you’ve got to document this technology stuff that you’re not all that interested in and that doesn’t exactly excite them, but it will save you a lot of trouble down the road right.

Roy: Right it certainly will. Also I have found that during that process, every person I’ve worked with has expressed how surprised they were at how much they learned from doing the process. That it wasn’t just another menial task.

Rob: Absolutely, you have an opportunity to examine how your systems are working together. You have an opportunity to find places where, “You know I don’t really need to use this particular piece of technology. I can make the system more efficient through the things I’ve learned going through this process.”

Roy: Right, so I think we’re at 11:05. Rob, I know you had to go and I apologize to everybody that this wasn’t as long as we promised, we probably could have covered more but I do think that we did get to at least cover the stuff we wanted to make sure you know about in this year.

Rob: Like Roy mentioned, there will be a bunch of resources linked to the presentation, there’ll be more information.

Roy: Those of you who registered for this show got 3 or 4 emails from me this morning as I was frantically trying to get the right link out to you. At least one or 2 of those emails does contain the resources links, also the web page that you could register from contains these links. The last comments about all this just to make sure we sum up
what's happening.

What we’re saying is, when we say you need a HIPAA fire practice for HIPAA compliance, really this was our way of getting you in here so we could say to you, this is HIPAA compliance, is you start with risk analysis, and then you do a risk management plan and then you implement that plan, and as Clinton is saying, this is an ongoing thing that you do. Clinton, how often would you say someone should re-up their risk analysis, like redo it?

Clinton: What we often work with within organizations, and these are very large systems so this might not ... This might be a little bit extreme for the private practice, but we often look at every 3 years, you go through all of your different security controls, you go through all of the different parts of your system. We can probably do it a lot quicker within a private practice than an individual that’s using a system.

What I would say is, once a year, you go through a good portion of what you've done over the past few years. You validate what's been done, you see if there's anything new. You look and see, “Do I have new risks? Have I added clients that are exposing me to the end type of risk or am I communicating in a different type of way?” Go through it that way.

I also think on a monthly basis or a bi-monthly basis, it’s useful to have a calendar of things you check your way through, and you plug your way back through. Once you finish your first round, start going through it again. The way I've been thinking about it in terms of how do we get a business model that actually works so that we can consult with small practices, because the way it's done for big enterprises and government is not feasible, costs way too much money and the model I think about is book keeping and accounting.

Every month you’re doing a little bit of work, checking your books, you’re looking at the new things you've done, you’re making sure they’re in line and that you’re following your processes. Then a couple times a year or once a year, you go back through and you have somebody look at all of it and make sure that it’s in good shape.

Roy: Right, that makes a lot of sense and I know a lot of people will probably wonder about, “Okay, so if I get to this risk management point, how do I know what to do?” I want to reemphasize that Rob and I ... This is actually why we write all these articles that we write, is because we know that there’s lots of these little details about different technologies that people don’t know, and so we end up writing these articles because we want to have that resource for people to look up, so they can see, “Okay, this is what these technical experts say I need to look for in my iPhone, iPad or in my Android phone or in my electronic health record system.”

That would be Rob, would be the one, the specialist there. That’s why we have those there, so when you’re ... If you want to try this process yourself or you want to ... Or do it with a group and then see how this is working for you, use our articles as a resource please, that's what they're there for. If you don't use them, there’s no point in us writing
them. Of course our newsletters are something that we use to keep people updated on changes.

There’s a ... It’s not just self-serving. Honestly, I use my newsletter to keep people updated on what’s going on. I know Rob does as well. We do honestly suggest subscribing to our newsletters as a good way to help yourself do these things that Clinton’s talking about, of keeping on top of things because we can help you stay informed when some important change in the world system happens, such as changes in HIPPA or when Google will suddenly start offering business associate contracts, we talk about that. These are important things that are useful to know. Do you have any comments about that Rob?

Rob: No, I think you covered it. Again, I’ll reemphasize your point that we’re putting that information out there, the more people we bring up to speed on things like this, the more we can tackle other issues.

Roy: Yeah, right. We can get past all that.

Rob: We can do every bit about half and then we can tackle bigger beasts.

Roy: Right, like I know parity or something crazy about [Crosstalk 00:42:11].

Rob: Oh that’s ... Oh my gosh.

Roy: Right, so we’re definitely trying to make ourselves unnecessary. I guess you could say. Rob’s like, “No I’m not. I want you to [Crosstalk 00:42:25].”

Clinton: I was going to say, maybe Roy is, but I'm ... I like to be necessary.

Rob: We’ll be necessary in new and inventive ways as we move forward.

Clinton: Yeah.

Roy: Yeah, I think that’s probably what it is. I’d rather be necessary in more ways than the basic ones.

Clinton: Yeah, right exactly.

Roy: Okay, I know you got to go Rob. Clinton, thank you so much for being here. I think we managed to get a 40 minute show, so that's not too bad. My apologies once again to everybody for the difficulties and of course, I'll be emailing out information. I had to watch the recording later if you didn't see the beginning, and yeah, good luck to you all.

HIPAA compliance, yeah, it’s another thing we got to do, but I think ... I hope that especially when Clinton was talking about it in the more philosophical sense, I hope you were hearing how the process doesn’t have to just be another menial task. It actually can be even an interesting experience. Good luck to everybody with that.
Rob: Yeah, thank you for joining us, Clinton.
Clinton: Yeah, thank you guys for having me. I appreciate it.
Roy: Sure thing. It was great.
Clinton: Woo.
Roy: Okay, I’m going to stop the broadcast and I’ll see you guys later.
Rob: Take care.
Clinton: Take care.
Rob: Bye.