FOLEY

FOLEY & LARDNER LLP

Health Care Law Today Podcast

Episode 7: HIPAA Risk Analysis 2.0: Duty of Care Risk Analysis

Please note that the interview copy below is not verbatim. We do our best to provide you with a summary of what is covered during the show. Thank you for your consideration, and enjoy the show!

In this episode, Foley Partner Jen Rathburn sits down with Terry Kurzynski, found of HALOCK Security Labs on the Duty of Care Risk Analysis, especially as it pertains to health care.

Jen Rathburn

Thanks, Judy, for the introduction.

Hi, my name is Jen Rathburn. I'm a partner at Foley & Lardner and I've been practicing for almost 20 years in the area of data privacy and security. I actually started my career in health care, focusing primarily on HIPAA, and over the years, I've expanded to working in all industries. I'm here today to talk about this podcast, and we're going to focus in on the Duty of Care Risk Analysis, otherwise known as DoCRA.

Today, we have Terry Kurzynski with us. He is the founder of HALOCK Security Labs and he's a contributing author of the Duty of Care Risk Analysis Standard, aka, DoCRA. The DoCRA Standard has been incorporated into the Center for Internet Security Risk Assessment Method, CIS RAM, and has prevailed with judges and regulators. Today, we want to explore what DoCRA is and why you should care.

Terry, welcome.

Terry Kurzynski

Welcome.

Jen Rathburn

First I wanted to do a little bit of a background before we jump into DoCRA. Being a health care lawyer—and many of you who are listening to this podcast are health care lawyers in this space—we've had the HIPAA Security Rule around for a long time. When it first came out in the 2000s, we all were like, “what is this HIPAA risk analysis of what we need to do?” And over the years, the OCR has really focused in on whether an organization has conducted a thorough risk analysis, and what have they done with the results? What are the risks and vulnerabilities that come out of that risk analysis and how have they addressed that through a risk mitigation plan?

In fact, this really is the foundational thing that a covered entity or business associate needs to do in order to be HIPAA compliant. Where we've seen this come in is that, post-breach, we know the number one thing that the OCR is going to ask for is, please give us a copy of your most recent HIPAA risk analysis, and what is your risk mitigation plan to address risks?

That's the backdrop. That's been around for many years, and I've worked with many, many clients over the 20 years to figure out, what do we need to be doing for HIPAA risk analysis? The OCR has actually even come out with guidance in a newsletter about what the difference between a gap analysis versus a risk analysis. Are we just talking about gaps or are we talking about analyzing risk? I do think that many organizations either did it internally—the OCR has some tools available online—or they hired an outside IT firm such as yours to come in and do a risk analysis. That's kind of how we've been going along for years, but nobody really knows exactly what we should be doing with our risk analysis, other than the guidance the OCR has to follow NIST.

I'm so excited today to talk about really HIPAA risk analysis 2.0, and what is DoCRA, and how does it fit into this HIPAA framework. So if you could just start out and kind of give us a little background about where DoCRA came from.

Terry Kurzynski

If we go back a little bit in information security, let's say to the '90s, the world was very much focused on controls. When the HIPAA Security Rule came out, organizations looked at it, and the first thing on there is a risk assessment. They promptly ignored that, because it seemed difficult, and they went right to the things that they were comfortable with, which were controls. They put in controls, and in fact, they even put peer groups together to talk about which controls the peers had in place, because they were really worried about, as long as we're doing what everyone else is doing, we're probably going to be okay.

So they get these peer groups, they started talking about all the controls they had in place, and then the consultants got ahold of this because they realized they can monetize, somehow, helping organizations with HIPAA compliance, so they did gap assessments. They skipped the risk assessment. They simply did a gap assessment between what is in the HIPAA Security Rule and what the organization was doing. They said, you have a maturity, or you have a gap, in these specific control areas, and the reason why is it was easy for consulting firms to train groups of young college grads on how to go out and perform these gap assessments.

Jen Rathburn

And lawyers. I actually did that, it was part of my beginning of my career. It's like, you don't have this policy or procedure? Gap, gap, gap.

Terry Kurzynski

Gap, gap, gap. Right, and in my profession, the information security profession, we've really done a disservice to organizations all these years because we weren't really following what the regulators and what judges ultimately were looking for if from a negligence perspective. But the reason why the HIPAA Security Rule includes the risk assessment as the very first item, we have to kind of go back and trace our roots back to 1993. Bill Clinton signs Executive Order 12866; we just had 12 years of Republican rule, and everyone's worried that we're going to be overly regulated, but he signs this executive order, which at its core basically says that all federal regulations going forward need to have a cost-benefit analysis.

All right, so the Office of Management and Budget interprets Executive Order 12866 as a risk assessment being required in all federal regulations, and we see promptly in the HIPAA Security Rule that it requires a risk assessment, and this is solely because of executive order 12866, but no one realized why it went in there. They just thought it was another control; perform a risk assessment, then we move on to number two and three and four.

What happened was, I started doing some litigation support about eight years ago for some of the largest cyber breaches on the planet to date, and as we're litigating these cases, it became really clear that what the judges were concerned about was way different than what we were basically prepping organizations to do. As attorneys out there, they're very familiar with things like the hand rule, calculus, and negligence, but as an information security professional, I'm like, wow.

Jen Rathburn

And why are judges asking me about this duty of care?

Terry Kurzynski

I'm like, wait, so he's asking about negligence? He's not clear that there's this encryption and all this other stuff, and that their SIM is in place and that they actually have multifactor authentication. He's going down a different route. Really what it comes down to is we, as information security professionals, we didn't know what the law knew, what the attorneys knew, was that the function of negligence starting in 1947 with Judge Learned Hand—I'm sure all the attorneys learned it in college—but was the threat foreseeable? Or the harm? Was it foreseeable? What was the gravity of the injuries, and what would the burden have been to you to actually do something about it to reduce it down to an acceptable level was sort of new for information security. We had never seen that before.

Jen Rathburn

And I would say fair. Most lawyers that are doing in-house compliance work that are the HIPAA lawyer in-house, weren't looking at it necessarily from that perspective. Because you've got to remember, when the HIPAA Security Rule came out, there wasn't a lot of breaches. It was more about, how do we figure out the

risks and vulnerabilities in our internal environment? When people were doing risk analysis, I don't really think they were thinking as well about direct foreseeable harm to third parties in the same way the judges ask about that in a court.

Terry Kurzynski

It was only a few years ago that OCR actually started doing their audits too, right? We're talking less than 10 years, even though the HIPAA Security Rule came out in '96.

Jen Rathburn

Final, in the early 2000s, yeah.

Terry Kurzynski

We started seeing breaches, because information became monetized, especially health care information became monetized in the last 10 years, so now we see the breaches, we see the lawsuits, and then now we see negligence, and we see fines. Even organizations that say, I'm HITRUST-certified, I have this, it didn't matter because they weren't performing the risk analysis for the foreseeable harm that could have happened. That was the big head-scratcher, the a-ha moment, wow, there's this other thing out there.

Jen Rathburn

And on that point, I think that that is really, really important, because I would say, as a lawyer, what clients ask me all the time is, what is reasonable security? What should I do? Just tell me what I'll do, I'll fit into a safe harbor, and we know that several years ago, Kamala Harris actually came up with what reasonable security was when she was California's attorney general, and she referred to CIS Top 10-SANS Top 10 as reasonable security. But I think it's really difficult for clients, not just in the health care industry, but any industry, to really figure out, what frameworks are we going to invest? You mentioned HITRUST. Or are we going to be ISO? What are we going to follow? Are we going to do NIST CSF? We do know the OCR does track online, both with the NIST CSF framework and the HIPAA framework, but there isn't clear-cut guidance to health care organizations, so in comes DoCRA.

Terry Kurzynski

The prep for this, once we were doing the litigation support, we realized that there was this disconnect. We started mentoring clients on how they could, because what we found is that the calculus of negligence, which then became the multi-factor balancing test for all the states—every judge, by law, has their multi-factors. Was the harm foreseeable? What was the relationship between the parties? What was the gravity of the injuries? What could you have done about it, within reason? They have their factors—they have their factors, they go through, and what we realized is that looked a lot like a risk assessment. If we tweaked a couple things in the classic risk assessment method—there's threat times vulnerabilities—we have a probability and impact calculation to get a risk score. If we tweaked a couple things, we could be meeting our duty of care, which we put us in really good regards with regulations and judges as well.

Jen Rathburn

So it's essentially a risk assessment—and when we use that term it means HIPAA risk analysis, because the marketplace really just says HIPAA assessment—but it's basically a risk assessment plus duty of care to a third party. It's not like you have to start all over from scratch, it’s adding on.

Terry Kurzynski

It depends on what your risk assessment looks like. If you're only doing maturity models right now on your controls, that's a start, because every risk assessment does have to model the maturity of your controls, but that in of itself doesn't tell me where I need to make investments in my controls. I have to do that based on risk.

Jen Rathburn

Or really provide guidance to the board of directors about where you should invest money. It's just a set of gap analysis, a maturity schedule.

Terry Kurzynski

As we evolved this thing and mentored clients, hundreds of clients, on this sort of duty of care concept, we had an opportunity to write the standard. That's where the CIS RAM and Duty of Care Risk Analysis Standard itself and a not-for-profit came up, and if you think about a risk assessment, if we do a couple things, we can allow it to meet duty of care. Right now, most risk assessments focus on the impact to an asset and to the organization. How does this impact me? What are the risks to me, the organization? What's the dollar impact to me? If you think about duty of care, we need to consider with our actions, how are we going to affect others outside the organization? Our risk analysis has to consider the harm to others outside of the organization, so that's number one.

We have to consider harm to others outside the organization, not just a score of risk to me or a dollar impact to me. In fact, I saw one risk assessment—large organization right here in Chicago, almost a billion dollars in revenue—and they wanted us to perform an information security risk assessment. We said, have you performed any enterprise risk assessments recently, because we want to look at the criteria, make sure we're congruent. They said, yes, in fact, we did, and they showed us the criteria. The criteria says, we will invest in risk remediation as long as it doesn't impact the bonuses of executive management.

Jen Rathburn

Wow.

Terry Kurzynski

So when you peel that back, when you really consider that, that really is the definition of negligence. I'm only going to do something as long as it doesn't affect my pocket book is not going to pass in the court of

law. When we revealed this, they quickly got rid of that and they replaced it with the concept of harm to others and we need to consider the harm outside the organization, that's step one.

Number two, we need to define an acceptable level of risk. What we've found is you've asked most CSOs or executive management, hey, what's your tolerance for acceptable risk? How do you define acceptable risk in your organization? And how do you think they would answer? Most would say, well, we sit around a conference room, we look at each risk and we basically give it a thumbs up or thumbs down whether we're going to invest in it or not. It's ad hoc.

Jen Rathburn

Or they do benchmarking up through the board, and the board ultimately makes the decision.

Terry Kurzynski

But at the board level, even, how are they deciding which ones they're doing are still ad hoc. There's not a calculus or a rhythm by which they're actually deciding on one versus another that actually is going to pass the muster in front of a judge or regulator.

We have to think about harm outside the organization, we have to define acceptable risk, and then we have to consider the burden of the safeguard. In traditional risk assessments, it's called residual risk. We wanted to do away with the term residual risk because, inherently in the term residual risk, it says that I'm reducing risk, which is not necessarily the case. So, we call it safeguard risk because the proposed safeguard that we want to put in might actually increase other risks in the organization, including a financial burden, by the way. I might solve the original problem, but I create another one.

Take a doctor's office, for instance, a patient portal. We had an organization immediately implement a two-factor authentication because they didn't have two-factor authentication for the patient portal for doctors from home to look up patient records. When they implemented it, it was a disaster because the doctors couldn't get access because they were using tokens versus some other form, and patient care was affected. The mission was more important than having this two-factor authentication from a security perspective.

Jen Rathburn

But that's so important because that's what the OCR has said for years, a difference with the HIPAA Security Rule versus the privacy rule is the security rule is scalable. There are things that are required standards and then some things are addressable, but addressable doesn't mean not do them, it means come up with a compensating control. That's exactly what you're talking about here, that if you're not going to implement a particular standard or control, at least you're documenting or thinking through the thought process of, what is that compensating control and what is the benefit or burden to the organization? And that aligns right in with DoCRA.

Terry Kurzynski

Yeah, so the risk assessment, if we do it according to the Duty of Care Risk Analysis, we can use risk to say of the required items, to what extent do I implement, and how do I know I've implemented them enough to reduce risk to an acceptable level? Not just acceptable to me, but all interested parties that could be affected or harmed? Then also for the addressable, which ones should I address and to what extent? Or which ones can I justify not addressing because the burden's too high and the weighted risk, or impact, is just too low?

Jen Rathburn

Can you give us some examples, like what you've seen in courts or what you've seen attorney generals look at from the sense of when an actual regulatory authority, or a judge, is looking at this DoCRA risk analysis, what do they say? What are they looking at?

Terry Kurzynski

We also perform litigation support for attorney generals for multiple states, so as they go after class action lawsuits, multi-state class action lawsuits, they gather the discovery of information, and the first thing we always ask for is the risk assessment. We know that the attorney general is going to be able to win the case if the organization isn't considering the foreseeable harm they could cause outside the organization. What is the mechanism by which they're considering the foreseeable harm outside? If they have a risk assessment, they might have a shot at it. If they don't have a risk assessment, they probably have zero shot at it, which we've seen case after case where organizations get fined because they don't have that proper risk analysis.

Jen Rathburn

I think that's really interesting and really important because I do not think a general health care regulatory lawyer is looking at a HIPAA risk analysis, per se, from a litigation perspective. I think this not only is a combination of health care regulatory law and IT security, but it's taking in the litigation end. For me, it really is HIPAA Risk Analysis 2.0. It's more of a comprehensive solution to help protect an organization, post-breach, to explain yourself to regulators.

And I will say that the clients that I have represented—and I do it almost on a daily, weekly basis, writing responses back to the OCR, other state regulators, clients that have a good story to tell—what you're saying is that we really, critically thought about what our risk is. We thought about not just our own selves and our own systems, but the harm to third parties, and we developed controls to do that. And we did an assessment in this way, has been, at least in my experience, very effective.

Terry Kurzynski

When you think about it, when you're in front of a judge, it's not because you hurt yourself. It's generally because you've hurt others, and there's always a control that you could have had in place to have prevented the breach. What the judge wants to know is, why didn't you have that particular control in place, and that calculus, this Duty of Care Risk Analysis, is going to be very necessary to show that we analyzed the risk, we prioritized the risk. This one was even on our list, but it was deemed low probability or low impact compared to these other things that we had made and are continuing to make investments in.

Jen Rathburn

Do you have another example of that?

Terry Kurzynski

If you don't have the story for how to back up the risk analysis, you're just not going to get it. We do know that of several cases where the attorney generals, upon receiving the risk analysis and the discovery of information, realize that organizations were performing a proper risk analysis that consider harm outside the organization, we know those cases were dropped. The attorney generals have told us of such, so we know that they're well-trained up now on this concept, and that the word is spreading even among the attorney generals on what to look for. We also know OCR is actually very skilled now in understanding the difference between a gap assessment, a maturity assessment, and a true risk assessment, meaning one that will consider harm outside the organization to the EPHI.

If an organization wants to have the best position to communicate to executive management on why they're making decisions on certain investments, if they want to justify in front of a judge why they had made certain investments, if they want to show a business partner, I'm considering the harm to you. If they want to justify to internal audit why we prioritize certain things, or if internal audit wants to help prioritize their findings, the risk assessment, and specifically a Duty of Care Risk Assessment, will allow all these parties to talk together and communicate in the same language.

The language we use in the risk assessment is not nerdy, techie security language. It's what's your effect and your mission, your objectives and your obligations or harm you can do others? You can have multiple missions, multiple objectives, and multiple obligations, we've seen one research hospital actually have 18 categories of mission objectives and obligations, because they have the hospital, they have teaching and then they have the research, so they have multiple things that they're driving towards.

This is in plain language that is viewable. In fact, I even have one organization that posted it on the web, like, here is how we look at risk. This is our mission, this is our objectives, these are our obligations, and they posted it right on the web for everyone to see.

Jen Rathburn

That's fantastic.

Terry Kurzynski

So, when clients want to do business with them or vendors or business partners, they can see how the organization operates. It's like this corporate social responsibility effort that's going forward. When you think about it, when we really look at the details, they say, we're going to consider our social responsibility. Well, guess what, they already had a social responsibility by law, it's called duty of care. The reasonable person translates to duty of care for companies.

Jen Rathburn

And that makes sense. Obviously, the technical security information, you wouldn't be posting up on your website to allow a hacker to come in. Not the vulnerabilities, no, but yes, your posture with regard to risk, and I think that's an excellent movement forward.

Let's talk just a little bit about, how do you get this risk analysis? How can you use this framework? In particular for organizations that are not familiar with ISO and NIST CSF, all these different frameworks, how would you use this in your organization?

Terry Kurzynski

First of all, it's all freely available as downloads. There's a standard, which is docra.org—D-O-C-R-A.org—and that's a not-for-profit organization that actually has the standard, but there's a detailed risk assessment methodology available at the Center for Internet Security.

Jen Rathburn

So it's all free?

Terry Kurzynski

All free. Download it for free. You can go to the Center for Internet Security and look up CIS RAM, risk assessment method, and you can download it. There's tools in there, there's spreadsheets, and there's a detailed step-by-step instruction, at least that we've been told, of any risk assessment method. The problem with most risk assessment methods that exist out there, including NIST 800-30 and ISO 27005 Risk IT, is that they're too generic. They don't actually give a detailed instruction of, how do I perform risk? It really leaves people kind of performing them in an ad hoc way.

We give the detailed instruction. You do not need to use the CIS controls to perform a risk assessment using CIS RAM.

Jen Rathburn

You can pick your own.

Terry Kurzynski

You can, and usually for health care, we would recommend NIST 800-53 controls, harmonize with HIPAA security controls. They're a little bit too generic, so you want to augment those with the 800-53 controls.

You can use the step-by-step instruction book, and there are tools and things coming out later, but this is all free. People can go out there right now and download it, put it in, and there's training available too.

Jen Rathburn

I think it's fantastic. I've recommended to a lot of clients. The way that we get involved with clients is, clients come to us and say, what do I do about a HIPAA risk analysis? As a lawyer, should I be involved in that process? How should I integrate with our IT team?

Terry Kurzynski

The Duty of Care Risk Analysis brings in legal and executive management in like no other because of the criteria piece. This calculated, acceptable risk definition, which is clearly spelled out in the CIS RAM download. It really involves executive management and legal, and the team, to decide on, what is our definition of acceptable risk? You're defining it upfront. What is your unacceptable hit to your mission? What's an unacceptable risk to your certain objectives about profitability or being number one or number two in your space or your growth plans? And then your obligations, what's an unacceptable hit? Is it five records of PHI? Is it 100? Is it 500? What's your threshold? And that's all going to be dictated based on your size and complexity.

Jen Rathburn

Where we work a lot with clients, you go through the risk analysis process, you come up with risks and vulnerabilities. Some of them you'll accept, other ones, you know you need to close those gaps and you have to develop a risk mitigation plan. And if you're not going to be closing those gaps, you need to understand why. Because what I see is, post-breach, regulators asking, well, this came up on your HIPAA risk analysis. You knew that this was a risk out there. You may or may not develop compensating controls. It definitely had a harm to a third party. I work with a lot of clients to help them develop the story, to make them understand what is per se required to look through acceptable risk, to do that under attorney-client privilege. But I think that the biggest advice that I tell, in particular, in-house lawyers is, really work together with your chief information security officer or your CIO.

This is not a simple IT, we've known for a long time now, cyber security is not an IT problem. It is a risk problem, but they really need to come together, in particular on the HIPAA risk analysis piece, because again, post-breach, number one thing that the OCR and other regulators are asking is, we want to see the risk analysis. We want to know whether you're a good or bad actor organization, and whether you did the analysis. I really appreciate all the effort that you and your group, and obviously others, have done to try to bring this integration between legal and IT security. I think it's a really valuable resource, a free one, that's out there.

Terry Kurzynski

Free. We already are required to do risk assessments, and if you do it, again, in a certain way, you're really going to get executive management, legal, and regulators real excited, and judges, everyone, on the same page. That's what we've seen over and over when you perform a proper Duty of Care Risk Analysis. It keeps everyone on the same page and it's business-focused. Too many times we see these vulnerability assessments or gap assessments that get too techie. Executive management doesn't know how to read that. How do they interpret that? How do they make a decision on what to do on that?

Jen Rathburn

CEO's and board of directors tell me all the time, I can barely understand when I come and get the report on cybersecurity. Let's be honest, a lot of people in those roles are older generation, they're not as familiar with technology. I always say, well, the way in which I present it and talk about it is really, what does this particular control do for you and how can it help protect your organization? But I think this type framework really takes out the techie-ness to really communicate with boards and the C-suite on these issues. I think it's a whole new way of talking about it because let's be honest, most organizations have a million different security vulnerabilities. It's a sinking ship. You have to figure out where you're going to invest your money in and you got to invest in the thing that's going to give you the best ROI for your dollar, that's aligned to your mission.

Terry Kurzynski

And no one expects an organization to instantly and simultaneously treat all the known risk once they're discovered. That's sometimes a pushback, right? I don't want to know what my findings are because then I have an obligation to do something about it. Yeah, you do have an obligation to do something about it, but only those that are reasonable, and you can prioritize those in a certain way that you can actually put them in over time.

Jen Rathburn

I would also say that too many plaintiffs lawyers do know these risk assessments are out there and they use them post-breach to try to prove an organization is negligent by the types of gaps they have. I get a lot of clients say, I get really worried when I do these because there's gaps that we may not be able to fill, and there's exposure that's out there.

Terry Kurzynski

It's funny you should say that. We've been brought in on a lot of post-breach OCR actions to perform an emergency DoCRA risk assessment. The risk treatment plan then is used as the injunctive relief by OCR. Fines are delayed, and OCR says, we'll see you in 12 months, make sure you're following your risk treatment plan that you put together because who knows better on which items to treat than the organization that just performed the risk assessment, a proper one.

Jen Rathburn

I suppose it shows the organization is taking it very seriously, doing their due diligence. They want to make sure that they're back into compliance.

Terry Kurzynski

Otherwise you have an outside agency. What control can they tell you you need to put in place? The best they can say is, perform a proper risk assessment. If you beat them to the punch and perform that risk

assessment, even post-breach, you can take control of the actions and the injunctive relief, if there's one coming

Jen Rathburn

Like LabMD and the FTCs ongoing battle of what were reasonable securities or not?

Terry Kurzynski

That was complicated, but at the end of the day, what surfaced out of that whole case was the FTC and the federal government don't have a definition of reasonable to the extent that organizations can actually use and run with it? But also, it was never the obligation of the federal government or regulators to tell specific organizations, this is your calculus, this is your specific level of reasonable risk that you need to operate by. Now, DoCRA gives all organizations, judges, and regulators a framework by which they can actually run some calculus. That's what it's doing right now. It gives them a framework by which they can decide their own calculus, so at the end of the day, organizations can take control of what reasonable risk is.

Jen Rathburn

I think it's fantastic. I'm being very serious about it. I think this is definitely a game changer in the space because it's bringing together all parties within an organization to make a reasonable decision about where they're going to invest funds.

Well, thank you again, Terry. I really appreciate this conversation today. I think it's going to be really helpful to many organizations, not just within health care, but also outside.

Terry Kurzynski

Go DoCRA.

Jen Rathburn
Go DoCRA. I'm going to turn it back over to Judy. Thanks, Terry.

END OF TRANSCRIPT