Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 12: "HEALTHeLINK, SHIN-NY, and High Tech: Safeguarding Clinical Data, With Drew McNichol"

Speakers: Kevin Szczepanski, Barclay Damon and Drew McNichol, Director of Technology and Security Officer, HEALTHeLINK

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live broadcast of Cyber Sip, practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Hey everyone. Welcome back to Cyber Sip. I'm Kevin Szczepanski, and we're pleased to be joined today by Drew McNichol. Drew has 30 years of experience working in information technology on an international scale. And for the last 10 years, he has been director of technology and information security officer for HEALTHeLINK, one of six health information exchanges or HIEs in SHIN-NY, the Statewide Health Care Information Network of New York. In addition to that, Drew participates in SHIN-NY's work group, which is designed to provide common standards and approaches to support New York's health care infrastructure. And for several years, he has been a member of FBI's InfraGard. Drew McNichol, welcome to Cyber Sip.

[Drew McNichol]: Hey, Kevin, thanks for that introduction. Glad to be here today.

[Kevin]: Oh, we're happy to have you, Drew. And we're going to talk today about HEALTHeLINK, what it is and what it does, certifications, and some of the lessons that you've learned in your 30 years in the health care and information security industry. But first, I want to talk a little bit about your background. What was it after 20 years or so that led you to join HEALTHeLINK?

[Drew]: Well, that's a great question. I think, you know, I've had a varied background in IT, started out as an application developer in the banking industry, was able to work in manufacturing, and got to see shop floor controls. And so multiple industries and an opportunity had come up later in my career—I also had done some consulting with software companies as well—but when the opportunity to join health care came up, it was really appealing to me because from a health care standpoint, if you think about it, we're all consumers of health care at some point in our lives. So rather than maybe just driving shareholder value, this was an opportunity to make a difference in the health care space where we're all consumers. So this was something to give back to the community and feel good about as far as my contributions. So when the opportunity came up, I jumped at it as well.

[Kevin]: I wonder how you feel about this, Drew, I've always thought in my experience with cybersecurity that the health care industry is really at the forefront and that industries that are trying to upgrade their own cybersecurity, manufacturing, for example, could look to the health care industry because some of the controls are the same across all industries. What's your reaction to that?

[Drew]: Yeah, I think, you know, health care is very highly regulated, whether it's federal or state requirements.

But one of the things that surprised me, Kevin, coming from banking and coming from manufacturing, was that health care at the time was a little bit behind where they needed to be with investments in cybersecurity. You might think because of the protection of protected health care data, that that would not be the case. But I found it was a little bit lacking in their cybersecurity program. So one of the things we're doing is we're borrowing from the banking industry, which probably has the highest cybersecurity because of the financial nature and for the investment that they make in it. So one of the things we had to do is really take a look at our investment in cybersecurity to make sure that we were keeping pace with tools and techniques that were available in the marketplace to apply those to the health care industry. So I would say that health care was a little bit behind the banking industry, but it's rapidly is catching up or has caught up.

[Kevin]: So let's talk a little bit about that now in the context of health information exchanges. Tell us more about what HEALTHeLINK is and then we'll talk a little bit about certifications and some of the lessons you've learned in your years of experience in the industry.

[Drew]: Sure. So happy to report that HEALTHeLINK is a health information exchange, as you said in your intro. And we've been operational for over 15 years. So this is not a startup type activity and HEALTHeLINK was started in the early days with a collaboration of the health care systems and the health plans in Western New York. It was really a unique experience; the CIOs in those industries got together shortly after HIPAA came out and said, rather than all of us investing in this, these requirements, why don't we fund an operation that could do this on our behalf? And that's kind of how HEALTHeLINK was born. But we collaborate and we provide clinical information in Western New York to the point of care at the provider locations. So if you think about the network here from a HEALTHeLINK standpoint, we're connected to nearly 100% of the hospitals. We're getting lab results and test results in on a daily basis we're getting encounter data from practices and we make all of that information available at the point of care for patients who have provided their consent to access that. And consent is one of the big components here that controls whether or not your information can be shared. And so if you think about it, we have we have over 315 million results that are part of HEALTHeLINK that we can bring to bear. And we get about 2.2 million results on a monthly basis into HEALTHeLINK. So that's a lot of data. And that data has to be protected and we have to instill the confidence in our community that that data is protected and only made available where it's allowed to be made available. So from that standpoint, HEALTHeLINK been in this business for quite a number of years and we're able to help bring to bear at the point of care better quality for the patients. Right, so the patients, if you think about it, Kevin, most patients have data in more than one medical record system. So if your primary care, specialist, maybe somebody else—and so how do you how do you get all of that information at one point to be able to treat the patient? This is where HEALTHeLINK comes in. We make those connections and we make that data available at the point of care to drive better patient outcomes and also to help make things more efficient and less costly in the market.

[Kevin]: Right. And so HEALTHeLINK is just one of six HIEs in New York. And looking at some of the statistics is... I knew we were going to be talking about it today. I think, as you mentioned, connects nearly 100% of hospitals in New York, over 100,000 health care professionals. And it represents is part of the SHIN-NY itself, millions of people living and receiving care in the state of New York. So tremendously efficient, tremendously helpful. But as you said, tremendously important then to ensure the adequacy of the privacy and information security safeguards.

[Drew]: Correct. And if you think about ... HEALTHeLINK operates in the eight counties of Western New York and as you mentioned, there's six what we call "qualified entities." To be able to operate in New York State, there's a set of policies and procedures that HIEs have to follow and we have to be qualified each year. So we are considered a qualified entity in Western New York operating in the eight counties. And we connect through the SHIN-NY that you mentioned earlier to the other HIEs across the state. So not only can we bring information from Western New York to bear, when we do a patient

record lookup, we can go out to the rest of the state and pull in data from other parts of the state. And we're also connected to one of the national networks as well, the eHealth Exchange. So we can go out and pull in veteran, VA data in about the patients. So if you think about it, it's like a network of networks where we're connected, interconnected on a secure manner to be able to bring the clinical data to bear where it needs to be, at the point of care.

[Kevin]: So to me, the implications for health care efficiencies and quality are obvious, but the risks are also obvious as well. Let's talk about the things that an HIE and a QE such as HEALTHeLINK have to do in order to be able to provide these services. I know that certification is critically important and I believe that HITRUST CSF Certification is preeminent. Can you talk to us a little bit about that and walk us through the process of certification because I know we talked before, it is not an easy process.

[Drew]: It is not. And we didn't start out having the certification. We've been operational for 15 years and in 2018 we received our first HITRUST certification. But prior to that, we had a very mature information security program. And so we were following guidelines from NIST and we would follow and have a very mature cybersecurity program that we had in place. All that was well and good. And then we started to take a look at, you know, with the industry changing and with these certifications arriving, are we missing something? Is there something in our cybersecurity program that we should … how do we take it to the next level, if you will? So we had started in 2017 to look at the certifications that are available, and there's a variety of them that are available out there. And we were heading down the path of a SOC 2 report and that's fairly technically focused about how you control your data. Do you have the right physical, technical, and safeguards in place for your organization? And right around that time, we were looking at the SOC 2, the state of New York, came and said, you know, if you're going to be operational in New York State as a qualified entity, we really want you to pursue HITRUST and we would like you to get certified on the HITRUST CSF. And so we shifted gears and we let the SOC 2 go and started down the path of HITRUST. And I've got to say, it's interesting because we thought we were pretty good about what it is we were doing, but we were really unaware of what it really took to do HITRUST. And I think our experience has been from the start. We undertook the initial assessment in 2018 and we probably had 300 to 500 controls that we had to have in place, meaning documented with policies and procedures and being able to pass an audit to show evidence that we were following those processes. And so we thought we were pretty good because we had many of those processes in place, but we lacked the evidence to show an auditor that it was done. And so this is where the formality started to come in, where we had to look at not only the job of an information security officer, but the rest of the company. What are people doing? How do we treat our documents? What did we do with the laptop once it's decommissioned? How do we destroy and dispose of the hard disk that might have information on it? Those types of things needed to be formalized and shown to an auditor to be able to show that these processes are in place. And so that changed a lot of what we needed to do. We put some more policy in place. We had to update our information security policies to have certain specifics added to them. And then we had to track processes on a daily, monthly, weekly basis that would show that we were doing the things that were part of our information security program. So that launched a whole new set of tasks not only for the security folks, but for everybody in the company who had a role in making sure that we became certified. And we achieved our initial 2018 certificate, the certification in 2018.

[Kevin]: So I'm glad you mentioned the safeguards, because I think when people think about cybersecurity, they focus on electronic safeguards. But as you mentioned, there are physical safeguards. What do you do with the laptop? What do you do with the physical documents you have? Where are your servers and how are they protected? And they're also legal safeguards as well, which I hope we'll have some time to talk about when we talk about vendor agreements. But I wanted to ask you about the controls, because I think a lot of people watching or listening might be thinking, all right, so there are 300 to 500 controls. What's the process for determine… for implementing those controls and auditing those controls? Do you rely on outside forensic specialists or are you able to do all of that in-

house?

[Drew]: No, that's a great question. And I should also mention that since 2018, the number of controls... and HITRUST you get certified every two years, you go through the formal certification and in the off year you do a self-assessment to make sure you're maintaining those things. And Kevin, our controls had grown to nearly a thousand controls we're recertifying on in 2018. So to your point, you have to have a process to manage that. And so, you know, we took a look at updating our policies. And we also have a bunch of procedures now that are ... we have a software tool that helps us manage those procedures. And they kick off and they remind us that things need to be done on a periodic basis. So in order to manage that large number of controls and be able to show evidence, I'll give you a quick example. So we do a lot of different software upgrades. You know, so our environment is fairly complex. We have a couple of different vendors we deal with to support the exchange and at the end of the day, they're making updates to that system, you know, on a periodic basis. And so we had to institute a very formal change management process that would indicate this is the vendor, this is the change we're making, here's what it's going to impact, and here's our back-out plan, if something were to fail. And so we would we had a robust change management system that was in place. But we when the auditor came and said, well, show me all the changes that were made in the middle of 2018, for example. Right? We're searching through email and we're trying to find ... so what we had to do is find a way and implement a change management program that would allow us to document and show what was requested, who approved it, and was it successful. So that closed loop process, so that it necessitated us looking at some additional software processes we had to put in place to really be able to manage the number of controls that we had in place and show evidence that they were being done.

[Kevin]: No, it's we did an earlier episode of Cyber Sip on the Three Cs of Cybersecurity for Vendor Relationships. And the third C was "comply," which of course I needed to have a C to make it three Cs, but that would really have really represented the audit process, actually making sure that you're doing what you say you're going to do in that off year that you mentioned for HITRUST, the year in which you're not getting certified sounds very much like a rigorous self-audit to make sure that everything you put in place the prior year is continuing apace in advance of that recertification process.

[Drew]: Exactly. And I also wanted to touch on something from your earlier question,

[Kevin]: Please.

[Drew]: You asked about resourcing and that type of thing. We're a pretty small team here internally, but we have over the years had a long-term contract with a cybersecurity firm here locally. It's somebody that we know and have used in the past. So they helped us build our cybersecurity program and make sure it's as robust as it can be and that we keep it maintained to modify with the bad actors out there, keep changing and we have to keep changing as well. So we rely on external experts to help us as well. And then we also hired them to help us with preparation for HITRUST. So prior to just calling up HITRUST and getting an assessor to come in and take a look at you, we did a self-assessment and we had the cybersecurity firm come in and help us with that. So there are external vendors that can help you through the process. And so we were augmented by our cybersecurity firm that we hired, and then we did an RFP to select who was going to be our auditor for HITRUST. There's a number of them that are out there and we had some specific things in mind that we were looking for, which was the right balance of them helping us and us helping ourselves. We wanted to play a role in that. So we also worked with an assessor that comes in and does that assessment period with you and then does the compliance component that gets submitted to HITRUST for the eventual certification. So we didn't do it on our own we had a couple of vendors assisting us throughout that process.

[Kevin]: I know you're in a highly regulated industry, but I think what you said is so important. I mean, you

are someone who has spent 30 years in the industry, director of IT and information security and yet even you will rely on external sources. I think sometimes smaller organizations, even mid-sized organizations, get caught up in thinking that, well, I have an IT person or I have an information security person in-house. I don't need to go outside the organization. And there's some reticence about doing that. Obviously, you do not have that reticence. What would you say to an organization that says we've got an IT person, we don't need to go hiring a forensic person to come in and review our systems; we've got that covered internally.

[Drew]: You know, that's interesting because some of the current thinking now is, you know, cybersecurity can be "solved." Right. My opinion on this is cybersecurity is not a problem to be solved because it's impossible. I think it's a long-term risk that you have to manage. And so while you might have an IT person that's getting the job done from an IT standpoint, the landscape, the threat landscape keeps changing. And so how do you keep pace on that? So I believe, you know, there's a lot of certifications around security. And if you hire the folks with the letters next to their name that know this inside and out, you can avoid, you know, expensive tangents that you might go in or pitfalls that you might run into thinking you're in good shape. And then next thing you know, you're not. So I'm a big believer in finding the value in folks that can help and do it in a cost-effective manner. They don't have to come in and do your whole piece, but you can give guidance on it. And one of the real good areas to leverage external help is in a risk assessment. You know, if you think about any of the certifications require you to do a risk assessment. And it's a little hard to do on your own because you might have blinders on in certain areas. So figuring somebody in from the outside who's got a question and it's going to take you through a very thorough risk assessment. It may only be a couple of days' worth of activity for somebody to take you through a risk assessment. And then at that point, management has the opportunity to say, okay, we found some things here. Which things are we going to follow up on? Do we have to allocate budget and over the next couple of years we're going to plug these gaps. You know, that type of thing is a very easy way to get started and it's not a very costly way either. But it gives you the information to know what's your risks and what you might need to do to help compensate for those.

[Kevin]: That's such an important point, Drew. One of the things that I find myself saying from time to time is you want to do the right thing for two reasons. First, it's the right thing to do. And second, if something bad happens later, you can say, well, I did my best to do the right thing. And the external assessments, I think, are evidence of how important that is. You want to be able to say, even if you don't decide to implement a safeguard right away. We had our internal team work with an external team. We thought this through. There were five things that we identified. We were able to do three right now; these other two are important as well, but here are the reasons why we decided to put those two things off. And if you can explain that rationally, you're in a much stronger position later on if someone, including a regulator, comes back and asks questions about that.

[Drew]: Absolutely. That's an important point because it's a defensible point. You know, ignorance of this, that control or the situation doesn't help you. That doesn't make it right. So if you show that you've thoughtfully done a risk assessment, it's up to each management team to identify how they assess risk. And that risk changes over time. So you have to refresh this and make sure that the threat landscape that changes, that your risk assessment follows that. And if you think about it, you know, the thing that we just have come through here, hopefully around COVID, it was two years ago, almost to the day, Kevin, where we were forced to close our doors and send everybody home to work. So when you're in IT and you're in security, that's a pretty scary proposition, because your landscape just changed. You're not worried about somebody coming in behind you to get into your building, to get into your suite. You're worried about what happens at home. Are people using their own laptops? Do they have the right security controls in place? So those types of things from a threat landscape has to be looked at periodically. And if you have somebody coming in to help you do that and you refresh that on a periodic basis, then that gives you the ability to say, look, we were aware of this. We did some

research on it. We assessed the risk. Here's the things we were able to do and here's our plans to go forward. That's a much more defensible position to show you are not ignorant of the situation and that you had plans underway to address it. Really important.

[Kevin]: That's a very critical point of discussion. And I want to ask you, we've got a little bit of time left, but will you come back and talk to us about information security in the remote work environment? Because I don't think that's going away across the board. And I think a lot of our listeners and viewers would benefit from hearing your thoughts on how to maximize your protections in a remote environment.

[Drew]: Yeah, I would welcome the opportunity to come back and talk about that. That's utmost on our minds these days, because to your point, I think we're going to be in this hybrid remote and in the office for the foreseeable future. So very important.

[Kevin]: So we talked about HITRUST certification, and you do that because the state requires it. But you also mentioned... I know you have an affiliate, HEALTHeNET and HEALTHeNET is not required to implement HITRUST, but it does implement other cyber protocols. Talk to us for a little bit about what some of the other standards are and how does... rather than HEALTHeLINK, how would an organization seeking to do business in the health care sector, or seeking to do business with an HIE such as HEALTHeLINK? How would an organization like that determine what protocol is most appropriate to hurdle that barrier of entry, so to speak?

[Drew]: Sure. And maybe just starting back on that HEALTHeNET topic and then just stepping back one step further, when I mentioned we work with partners that help us from a cybersecurity. Again, HEALTHeLINK was started by the four hospital systems and three insurance payers in Western New York. And we're blessed with the opportunity to have a security committee made up of the chief security officers of those organizations. So one of the things that we've learned from a security standpoint, if you raise the bar for security, it raises for everybody. So while these facilities, are competitors in the Western New York area, they also sit on our board and they... we share information. So one of the things that we looked at when we were looking at getting certified for HEALTHeLINK and I mentioned the state required HITRUST. Our security committee came to us and said, we know you provide the support for HEALTHeNET, but we'd like HEALTHeNET to go through an audit as well. We believe what you say that you're doing the same facilities, but we would like to have an audit of the HEALTHeNET application, which is the administrative data exchange that we support. And so we looked around, we had some options. NIST provides a framework, HITRUST does, and we were very familiar with that. But we also looked at ISO 27001 and our cybersecurity firm talked to us a little bit about that. And based on where we were and the scope of what was included in getting audited, we found that ISO 27001, which is based on the NIST standards, has all the same controls, but we could do it in a more efficient manner, meaning it was less costly for us and it took less of our staff's time to get through the audit. And I'm pleased to say that we've just achieved ISO 27001 certification for the HEALTHeNET application just in recent weeks.

[Kevin]: Oh, congrats on that.

[Drew]: Thank you. And so that was a lot more efficient to go through based on us having already done HITRUST. So I guess to the audience, there's a variety of different certifications that you can pursue out there. And I think a lot of folks feel that it might be too costly to go through one of these certifications. And if you think about it, you really want to take a look at, you know, balancing the scope of what it is you're trying to do with the certification level. So there's some pragmatism that you have to apply when you're looking at the scope of being certified.

[Kevin]: Well, great advice, Drew. I see we are running short on time and there are so many other things I

want to ask you about. You talk about remote work environment. We can talk about key points in vendor contracts because I know you have vendors and HEALTHeLINK is a vendor. I may prevail on you to come back and talk to us about that as well. But I, I appreciate that. I think there's a lot here and a lot to unpack. In our remaining moments, though, Drew, I wonder if you could tell us what are some of the lessons that you have learned in your last 10 years in the health care industry that you think everyone should know whether they are seeking to work in the health care industry or whether they're outside the industry?

[Drew]: No, that's a challenging question. I think, you know, if you look at it, when I first started my career, cybersecurity wasn't even a thing, if you think about it. And I remember opening up my first shrink-wrapped package that was an antivirus program, and I'm like, what do you need this for? Right? We are not connected to the Internet or any of that. So at this point, we know that cyber issues are real. And so some of the things that I've learned coming through is that you can't just chase a certification and say, you know what, I'm going to get HITRUST certified and I'm going to check all those boxes and then feel that that takes the place of an information security program because it does not. So you have to you have to spend the time to build a thoughtful information security program, starting with policies and procedures, standards that need to be in place, physical controls, technical controls, all of those components. And then once you have your IT security program established, then pursue that, the certifications. One of the things that I really learned going through this is that our information security program became better based on going through these. I was a little skeptical to say we're pretty much doing everything we need to do. We did find some things that we could improve, and it gave us the ability over time to improve that security program. So my view on it is, you know, be very pragmatic on what it is you're trying to do, have your information security program in place and then go in with an open mind around here's some things that are going to help us improve. And then you have to look at which things you're going to do that give you the benefit that you seek and things that might just be busywork, checking a box that don't give you the real pragmatic opportunity to improve. And I stated earlier, Kevin, you know, it's not a problem that can be solved. What it is, is a long-term risk to manage. And I think if you take a look at doing the risk assessments, as I mentioned, and then also keeping pace with the landscape and the threats that are out there, make sure that you have a long-range plan for your program. You may not be able to do everything in year one because of budget impacts, but lay out a roadmap and be able to progress so that when you look back two years, three years, four years down the line, you can see the progression. Don't get caught up in the day-to-day, saying we'll never get there, you know, that type of thing. So I think the longer term view is important and if you've not started yet and you're concerned about it by burying your head in the sand doesn't help. It's better to address it now and then start down that journey because it is it is a journey. And that's what I found over the last 10 years in health care, is that it's sort of an endurance sport that you have to you have to stay up on.

[Kevin]: That is great and invaluable advice. Drew, thank you so much for sharing that with us. And thank you for joining us on Cyber Sip. I hope you'll come back again to talk about some of these other issues. I think that your perspective and your advice not only to the health care industry, but to other industries that are looking to upgrade their cyber hygiene would be very helpful.

[Drew]: Awesome. Yeah. Happy to do so, Kevin.

[Kevin]: Well, thank you very much. Drew McNichol, director of technology and information security officer of HEALTHeLINK. Thanks to Drew for joining us and thank you for joining us. We'll be back soon with another episode of Cyber Sip.

[Kevin]: The Cyber Sip podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

Disclaimers:

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.

Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.