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

[Kevin]: Welcome back, everyone. We're so glad to be back with you in another episode of Cyber Sip. This is actually the last episode of Season 2 of *Cyber Sip*, so the next time you see us, yeah. So we're going to be in a new studio in January.

[Bridget Steele]: All right.

[Kevin]: It's got a really cool look. We checked it out. The paint is dry. The microphone is screwed into the table. So we'll show you more of that over the next couple of months. But really excited to be here today with this episode, which is "Don't Fear Compliance! How Health Care Startups Can Go From Zero to One." And this is our first episode, in two seasons, our first episode with two guests. So we'll see how this works.

[Ryan Young]: Wow.

[Bridget]: Really.

[Kevin]: But the three of us have done this before. We actually, this is kind of a redo of a live stream that we did for IBM on Z Day back on October 18. So joining us is the incomparable Bridget Steele, my favorite colleague here at Barclay Damon. She is counsel in the Health Care and the Data Security & Technology Practice Areas. Ryan Young is founder and CEO of Opollo Technologies, which is a fintech health care AI company. Ryan is a medical doctor and has his MBA, but in addition to medicine and business, check this out, he also has a background in quantitative finance, distributed systems, artificial intelligence, and medical natural language processing. Ryan received his medical degree from the Jacobs School of Medicine and his MBA from the University at Buffalo School of Management. Bridget, Ryan, welcome to Cyber Sip.

[Bridget]: Thanks for having us, Kevin.

Ryan: Thank you. Absolutely, I'm super excited to be on the podcast. Appreciate you inviting me.

[Kevin]: Oh, thank you for joining us. We had a lot of fun on Z Day, we had so much fun. We want to talk a little bit about what we talked about back then. So Ryan, as a founder of an early-stage health care startup, I think you quickly learned that you needed to demonstrate a compliance with data privacy and security laws to go from zero to one. We're going to talk about that. But first, why don't we tell everyone: What is Opollo Technologies?

[Ryan]: Yeah, absolutely. So Opollo Technologies is a fintech health care AI company. Our main product is the Opollo ecosystem, which is comprised of two components. Opollo, which is an AI algorithm, which provides more accurate switch duration forecast in minutes. And then the Opollo exchange, which is a marketplace

Episode 47: "Don't Fear Compliance! How Health Care Startups Can Go From Zero to One"
11.15.23 | *barclaydamon.com*

BARCLAY DAMON LLP

for health care facilities to sell medical services to insurers. And the great thing about the Opollo ecosystem is, as Opollo frees up additional time slots, right? That allows the facilities to actually sell those on the Opollo exchange in the marketplace and monetize their efficiency and further increase patient access to high-quality, low-cost health care. So that's super high-level view. Love to really share more with you guys about our journey and actually how Barclay and well, a little spoiler—and IBM also has helped us along the way too. So, yeah.

[Kevin]: Yeah, no, we know that. But before we move on, so what I'm hearing you say is, Opollo makes the surgical process more efficient. It saves time and then enables the providers to sell that time you save to perform more surgeries. So it sounds to me like what you're doing gets more people into surgery faster and really streamlines the health care process.

[Ryan]: Exactly, exactly. The idea and the concept is by, again, freeing up the time, you have now an additional, let's say, 60-minute block because of the inaccurate forecasts that are currently going on with the existing systems. That block would just sit dead. There's no activity. Because of that, that means an initial patient couldn't receive care. And also, 70% of hospital revenue is actually from the surgical operating room suite so it's incredibly important revenue driver; or for an ambulatory surgery center it's 100%, or near 100%. So making sure that they can more effectively plan so that way and utilize a very valuable resource and maximize it out. But also again we don't... by providing its forecast in minutes right it's not like we're telling a... someone who's been a nurse for like 20 years, okay, you need to make sure you take your break at 12 p.m. instead of at 2 p.m., right? And so we are able to reduce the workflow changes that are required instead of just swapping out the number.

[Kevin]: No, it's terrific business and I wanted to underscore that. But still, I mean, you are... the title of our episode is "Don't Fear Compliance." And... so you're a startup working for an industry, health care, that is laser-focused on compliance. And talking about getting from zero to one, you're not going get in the door. You're not going go from zero to that first client unless you demonstrate it. So what...What were, we know startups face a lot of those challenges early on. Ryan, what were some of the challenges that you faced in your initial foray into the health care industry?

[Ryan]: Yeah. So again, it's startups and I can speak for any [inaudible]. You have a really innovative solution, but you're operating in an industry that has more risk averse customers. Again, health care data is... it's we've got federal laws protecting it, right? With HIPAA. And so that makes those prospective customers a little bit more, again, they're risk averse because they're like, well, we like your idea, but we try it out, even if it works great, like a couple of weeks later, we see that there was a breach, well, all of a sudden now we are inviting in a lot of, because there's federal laws, like federal investigations, and then we're damaging our name brand. And so for a startup, right, a lot of those risk adverse customers more prefer to work with the larger established brands. And...So really, to really try and break through you really got to show that you understand both the compliance side as well as the IT/security side and be able to show them, yes, we have a great innovative product, but here's how we protect your data. We understand the compliance and that's a really important thing because although operations would really want to use your product, again, legal as well as IT/security, they do have...they each have their own ultimate veto on anything on your product. So you got to really satisfy both of them.

[Kevin]: So in thinking about that and confronting that challenge, what did you decide to do? How did you bridge the gap to ensure that you had those security controls in place?

[Ryan]: Yeah, really on the legal compliance side, it really comes down to how Barclay Damon really helped us. And I'm sure Bridget can talk a little bit more background on what she was doing, but really working with her with consultations on, okay, here's your HIPAA manual, it's like 100 pages long, and we really use that as our sword and our shield. But working with her week in, week out, going through the...the actual policies that are listed in there, making sure our tech stack works with along with that. It was incredibly important because

Episode 47: "Don't Fear Compliance! How Health Care Startups Can Go From Zero to One"
11.15.23 | barclaydamon.com

BARCLAY DAMON LLP

then we can then go in front of the lead compliance officer at a health care facility and say, hey, yeah, like this is what we do, this is how we protect your data, here's our policies and procedures. Also, because we're using IBM Cloud and IBM Hyper Protect, those policies and procedures, here's actually how we're actually protecting your data or we're using IBM Hyper Protect, which is...the Fort Knox of data security. And so when Opollo is reading and interpreting clinical notes using that medical natural language processing, we're doing that in IBM Hyper Protect, and it's really, it's a secure enclave that even IBM can't even access. And so we can show that this is, that data is being processed in a safe and secure manner. And then flipping back to legal compliance, we can then say, when the data leaves, that secure enclave. it adheres to the HIPAA Safe Harbor De-identification Method, which means it's no longer considered PHI, protected health information. And because of that, [people from] compliance say, well, yeah, that's great. That's exactly what we like to hear because we know that again, our data is being safe and we're willing to try out an innovative solution by a startup. So again, it's really both aspects are incredibly important.

[Kevin]: Mm-hmm. So you're able to say that to get that first customer, you're able to assure the health care provider, we have built information security into every step of the process. And that's so important, I'm going to come to you now, Bridget, one of the reasons that's so important is because the health care provider has laws, including HIPAA and perhaps high tech to comply with. So for those...of our startups out there may be thinking, well, I'm not a covered entity. Why do I have to apply, comply with HIPAA? If you're working for a company that itself must comply, you need to as well, or that company, that provider is going to go to someone else. So let me go to you, Bridget. To me, compliance means that your startup needs a lawyer. How did you start working with Opollo Technologies to provide that layer of legal protection?

[Bridget]: Sure, Kevin. So yeah, I met Ryan. I mean, Ryan had been working with our firm on getting his startup set up and he had this product. He had this great idea and he wanted to, you know, find a potential pilot partner to test his product out in the real world. And so he was starting to talk to potential pilot partners. And when we met Ryan was...very serious about making sure that he had the right policies in place. That he understood them, which is nice and refreshing. Um, and that they were tailored to his tool and that, you know, when he went into the business team and, you know, made it through a few rounds, he could then go in front of the legal compliance folks at these hospitals or health systems or wherever, and be able to kind of speak their language and show them like, no, we, we take data protection very seriously. And so, we, I sat down with Ryan and some members of his team and just made sure that his HIPAA policies and contracts were tailored. And when you're working as a startup, it's a little bit different. Like Ryan's saying, a lot of providers have checklists. And they expect you to be an extremely mature organization. And you have to show that you can play in that sandbox, especially in the health care space. But, Ryan was able to get himself set up and working with us and, honestly, just putting the work in day in day out to be able to have those conversations with the compliance folks. And that I think goes a long way in being able to like you were saying, go from zero to one customers and then build your customer base out. Because you really need to take compliance seriously from the gate in the health care space if you want to be successful in being able to gain the confidence of providers that have a lot of regulatory obligations that they need to comply with.

[Kevin]: And so I'm thinking, and I want to get your reaction to this. I think, Bridget, a lot of, or at least some startups and other businesses see lawyers as an obstacle. These are the people that are going to come from outside, they're going to slow everything down and we're not going to be able to do what we really need to do, lickety-split. And I think that's wrong. But I wonder your reaction. To me, the lawyer is a partner that works with the startup every step of the way to make sure that legal compliance is built into each of those steps. Is that right? Or how would you explain that when you're talking to, and obviously we have Ryan here, but when you're talking to the Ryans of the world, how do you sell them on the importance of building legal compliance into the process?

[Bridget]: Yeah, so just like you said, I see it as a partnership. You're trying to help your client be successful. I mean, I think with Ryan, it was a lot easier because Ryan took compliance seriously from the get-go. So there wasn't a lot of persuasion there. You kind of got it, right, which is good. But as a startup, you aren't going to

Episode 47: "Don't Fear Compliance! How Health Care Startups Can Go From Zero to One"
11.15.23 | barclaydamon.com

BARCLAY DAMON LLP

be the same as an organization that's been around for 30 years. So you have to be practical and pragmatic when you're counseling startups and making sure that they have what they need to get themselves through the front door. But also understanding, meeting them where they're at, and being able to take the time to do the consultations, walk through what they're really doing and understanding like with Ryan, like he was saying, you know, they were actually, they do de-identify a lot of the data in their tool. And so even being able to kind of coach them on how to talk about that process with potential partners and then kind of... that does kind of mitigate a lot of any concerns about risk. So really, customized legal counseling and advice... and that's I think how I view a partnership is really getting to know your client's business and what they're doing and helping them succeed.

[Ryan]: And in Bridget's consultations were helpful in terms of, again, us going back, revisiting our source code and saying, okay, well, how can we actually have Opollo process PHI, but not store it? And there was actually a rewrite after we had met with Bridget several times. We said, okay, well, we can really follow like the HIPAA safe harbor guidelines and say, okay, well, we were storing at the time, we were storing like ages that were like 92, which is technically PHI. Now what we store is as long as the age is below 89 years old. So there's a hard cap at 88.8888 so that way... the reason why it's point not .9999 is a floating point error. Again don't necessarily need to explain that highly technical thing. Let's say like on a trial witness stand right so that's why we keep it at 88.8 because it's not going to ever round up an entire you know .1 right it's but if you made it like seven nines afterwards then it could might round up just because there was a floating point precision error. Again, this is computer science stuff, but understanding that you can put that into code so that way you're now making sure that you're in compliance and then also you're doing it so early on in your company that you don't have to go back and do this stuff again. Right? You just did forethought, right? Yeah.

[Kevin]: Yeah, to me, it just ...sorry to interrupt, but no, thank you for that. I think it just underscores the importance of integrating the science, the technical with the legal and doing it from the gate, as you said, Bridget. Okay. So let's turn to what you actually did. Um, how you implemented the security controls to achieve legal compliance. And this is not a spoiler alert, but an alert. There are many different ways to do this, and there are many great vendors that provide services like this. We could talk about Amazon, we could talk about Microsoft, but I know Ryan, the choice that Opollo made was to go with IBM Hyper Protect. So I know you're going to be talking a little bit about that. This is not a commercial, for those of you watching or listening, but I think the reality is there are a number of different choices, and I think it's important to hear Ryan's story of how he made his choice. So...Let's go there now, Ryan. So what types of technology did you integrate into your startup in order to achieve the legal compliance targets that you needed to in order to get your first customer?

[Ryan]: So we were, Opollo Technologies was accepted into the IBM Hyper Protect Accelerator. One of our advisors, James Gillespie, had suggested that we apply and we got accepted in, which was great. And Adam Ring and his team have been fantastic. Adam is the global head of the accelerator. Really getting to understand the... IBM's technologies. Also, IBM is such a trusted brand name. Like every large corporation, again, a lot of those risk adverse customers, they have IBM mainframes in the basement. And so just that alone and then on top of, okay we're using a lot of IBM's technology to actually secure the data as well. So for example we use that secure enclave, it's called the IBM Hyper Protect virtual private cloud and again it's a place that runs in an IBM Z machine where it's a secure enclave that even IBM doesn't have access to. So we can process all of the PHI there. So when Opollo receives the clinical note and it's got to run the medical national processing on that note, by doing it in the actual IBM Hyper Protect virtual private cloud, we're able to actually make sure that the data remains secure during processing. And then at that point, you know, we've de-identified it. And then when it leaves, it's been de-identified, it's no longer considered PHI. We also use IBM Hyper Protect [inaudible] services. Again, that's now, even though the data's been de-identified at this point, right, we still want to protect it, right? And so we want to use those keys to actually, those encryption keys to actually then continue to secure that data when it actually is, after it's left the virtual private cloud. And we actually are going to store that non-PHI. We still want to encrypt it. And so we do that afterwards. And so those are the two main ones. There's another feature IBM's getting ready to roll out in the next, hopefully

Episode 47: "Don't Fear Compliance! How Health Care Startups Can Go From Zero to One"
11.15.23 | barclaydamon.com

BARCLAY DAMON LLP

sometime Q1 2024, again, in health technologies, we're excited to be a part of their beta tests. So that's all I can say for right now, but we're looking forward to testing it out next year.

[Kevin]: Yeah, no, that's super. I want to come back to you in a second, Ryan, but Bridget, you're hearing this, and the question I have for you is, what's your thought process? What's the analytical process when you hear that Opollo or another client is employing some technological platform in order to achieve certain security controls? How do you evaluate that to determine whether those controls comport with the client's legal obligations.

[Bridget]: Yeah, I mean, a lot of providers in the health care space are looking for, at a minimum like a SOC 2 or high trust certification or some level of security certification that's a standard that has security controls tested against it. So working with vendors that are as well-established and have these kinds of certifications in place, you can just automatically get a lot of confidence in doing that. And so, you know, not every vendor has that, but then, making sure there's contractual obligations in place and make sure they're meeting certain controls. And yeah, the end goal is just to make sure that you're protecting data that you either are housing or processing, in compliance with law and honestly beyond the minimum obligations, because in today's world, the security is huge. And especially if you're a service provider or vendor looking to maintain your client base or grow.

[Kevin]: Yeah. So can we talk a little bit about vetting vendors? So Ryan, you made a strategic choice to implement the IBM Hyper Protect program. There are other vendors, large and small—without turning this into a commercial, which we don't want to do, but talk about how you made that choice. I mean, you obviously know there are many alternatives out there: local, regional, national, international. Why did you decide to make the choice you did? I think it would be helpful to our audience to understand why you went, I'm going to say why you went big, as opposed to just using the local IT or information security firm that many of us use every day and find very effective.

[Ryan]: Yeah, so we actually, we originally, prior to getting into the accelerator, we were in AWS and then we migrated over to IBM Cloud. What made it relatively easier to switch for us was, again, we… a lot of the really, and this is our chief technology officer, Pete Turner, as he was reviewing IBM's tech stack, he noticed there was a lot of similarities. So for example, S3, think of it as a distributed system version of like a hard drive, right? So basically many computer, many servers like sharing, basically that own a hard drive. So Pete started to, as he was digging through it, he's like, oh, okay, you know what? I'm seeing S3 in IBM Cloud. So it makes it a little bit easier for us to actually migrate over because there are, you know, they're using a lot of the open-source technologies that are, that, you would may expect from other cloud providers. Also, again, the addition of IBM Hyper Protect in terms of actually being able to say, this is how we're actually securing your data, risk averse customer, as well as, again, just having access to the accelerator program is fantastic, pretty much I can send one Slack message to Adam and in 24 to 48 hours, we've got an actual IBM engineer that… had written some of that source code that we're asking questions about. So being able to have access to that, it just made it a no-brainer just from the level of support from the accelerator. The great tech stack that they have, IBM is a very well-trusted name. They do have for a lot of their services, high trust certification. And we, of course, again, have talked about Bridget, we've saved a lot of that stuff too. So that way we're able to review it and see what hits it. And …Which also is great for us too because when we are ready, because high trust is expensive to get on your own. So as an early-stage startup, right, getting everything in place now. So that way when you get to actually going through the high trust certification process, you've got all your ducks in a row too, from just again having those conversations about exactly how you're securing the data, how, because we talked a lot about with Bridget, well, okay, well, how are we monitoring this? Like, are you having a place where you can actually store these logs and provide evidence to back up that control? So by having a lot of support in place, it'll also help us down the road too.

[Kevin]: Right. So no, that's… and that makes perfect sense. And I want to turn back to you, Bridget, we've got a little time left. You're hearing this and IBM is a trusted vendor. There are other trusted providers out there

Episode 47: "Don't Fear Compliance! How Health Care Startups Can Go From Zero to One"
11.15.23 | barclaydamon.com

BARCLAY DAMON LLP

too, including Amazon, Microsoft, there are others. As a lawyer, and I think in this case it was a little, it was special because Opollo had already selected its vendor by the time you got involved. But when you're working with startups, who haven't done that. How do you talk to the startups about vetting their vendors to make sure they have the right company in place to provide that information security and the controls they need to achieve that legal compliance?

[Bridget]: Yeah, I mean, like I said earlier, you look at whether they have any certifications, you look at their, Kevin, you know, their cyber insurance policies and practices. You can even do some due diligence in asking them to complete questionnaires, or if you want, if this was a serious engagement and you needed to do a assessment in advance, you could see if they were willing to undergo an independent assessment by a third party. There's a lot of different approaches and it really depends on the nature of the project and how large of an obligation you're undertaking in using a certain vendor and what the risk is. So everything's always kind of wing: risks, benefits, current situation. I mean, Ryan, a perfect example, like high trust certification, it doesn't. It's not going to necessarily make sense for an initial startup to get a, to get high trust certification, even if there are some providers who would expect that or almost, or require something similar to that, just because, it may not make sense if you're just getting off the ground and the amount of money costs, not inexpensive. So you're always making those, you're, you're giving legal advice, but you have to understand the business side and the technological side and the reality supports going on. So there's always a lot of balancing and trying to understand your client's specific situation and also the nature of what they're doing and what the risk is.

[Kevin]: Yeah, no, I think that's right. And so I mean, I think one takeaway certainly, and that's super helpful, Bridget, one takeaway from that is, yes, your vendors are third parties, they're separate entities, you have contracts with them. But for purposes of compliance, think of your vendor as... your vendors as your right arm and your left arm, because ultimately, you are even if you're delivering services through your vendors for purposes of legal compliance, your vendors are you, and you are your vendors. You're ultimately responsible for that.

[Bridget]: Yeah. Yeah, and Kevin, I'll just say one more thing on that point. I do a lot of work on the health care provider side as well, working with clients like Ryan. And yeah, vendor management is huge right now. And there have been a lot of attorney general and other cases where providers have been dinged for basically missteps of their vendor.

[Ryan]: Yeah, yeah.

[Kevin]: Mm-hmm.

[Bridget]: ...not knowing what kind of data they have and not really taking inventory of that. So it is super critical in a lot of compliance programs and we have a lot of health care provider clients who are cracking down on their vendors in that respect.

[Kevin]: Yeah, we're seeing that. All right, so we've got less than a minute left. In that final minute, I want to turn back to you, Ryan, and have this question. So you've achieved this measure of compliance, you've gotten from zero to one. When you're trying to go from one to two, or one to 10, what story do you tell to your potential customers about your legal compliance and how does that...strengthen the case that you can make to potential customers.

[Ryan]: Yeah, well, it's really important for, again, another way we can further accelerate growth is by meeting with larger companies to strategically partner with them. I just yesterday had a meeting with a large consulting firm too, about what we're doing and what we're interested in, but saying, hey, this is ...sending them our – because we keep that HIPAA manual in our sales packet. Okay, these guys are pretty serious because they've got that 100-page HIPAA manual there with the policies and procedures, and then talking to them about how we secure the data using IBM's technologies, and weaving that into a strategic partnership discussion. Again,

Episode 47: "Don't Fear Compliance! How Health Care Startups Can Go From Zero to One"
11.15.23 | barclaydamon.com

BARCLAY DAMON LLP

they're a large firm that are well trusted by their clients. And so they're looking to make sure that... we have a very interesting concept. But again, it's that we only want to introduce our clients to the very best. And so by saying, hey, this is a...a good company that they dot their Is across their Ts. They're surrounded by a great firm that has really helped them in terms of being able to understand and then being able to go out and actually implement a lot of those technologies to make sure that we're hitting that level of compliance and IT security. Again, gives them greater confidence, allows them to feel like, okay, this isn't your early-stage startup. You know, they're operating in a much more mature stage then... which is great for us because that means again getting that risk averse customer to help and then bringing in strategic partners who are saying, "Oh yeah I want to show this to these other ours clients of ours because they trust us and we can clearly see they know what you guys are doing here is you know we know that you guys are going to be a good shepherds of our customers data." So. All that goodwill again is really how you can really get that parabolic growth and really lift off. So we're looking forward to the next six to 12 months here at Opollo Technologies.

[Kevin]: Yeah, I'll bet. I mean, you have not feared compliance. You've embraced it. And I think that's enabled you to demonstrate your competitive strength with clients and, and we're grate... It's great to have you on and wish you continued success. I know we'll be talking more in the future, but I wanted to share this story with our audience because you needn't fear legal compliance, but it is important. And if, as Bridget and Ryan talk about, if you weave that into every step of your development process, you're going to be in a much stronger position to go after business. And your competitors who have not done this are not going to succeed because the health care industry is too mature. It is too conservative when it comes to legal compliance, data protection and security. So...Dr. Young and Bridget Steele, thank you so much for joining us. It's been great to have you on today.

[Bridget]: Thank you, Kevin, that was awesome.

[Ryan]: Thanks again for having us. I appreciate you guys letting me onto your platform. So I appreciate it.

[Kevin]: Oh no, we love to have you on. What a great story it is. And I will just say we've enjoyed season two of Cyber Sip. Ryan joining us for the first time, Bridget, her second appearance on the podcast. We've got to give you some certificate or something for that. I don't think we have one, but we're going to make one up just so you have it. And I hope you, we should, you should come back in season three and we should talk about a compliance checklist for startups. I think that would be super helpful.

[Bridget]: Yeah.

[Kevin]: All right. Well, thanks to you, Ryan Young and you, Bridget Steele, and thanks to all of you for joining us. We've had a wonderful second season. I want to thank Maureen Fyke, Irene Meyer, and especially Kyla Handley for her invaluable production help. None of this would be possible without those wonderful people. And we're looking forward to working with them in the coming season. So thanks very much, and we'll see you in season three 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.

Episode 47: "Don't Fear Compliance! How Health Care Startups Can Go From Zero to One"
11.15.23 | barclaydamon.com

BARCLAY DAMON LLP