Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 4: "Cybersecurity in Health Care: Five Steps to Compliance, Featuring Bridget Steele"

Speakers: Kevin Szczepanski, Barclay Damon and Bridget Steele, Barclay Damon

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

[KS]: Welcome back to the Cyber Sip podcast, I'm Kevin Szczepanski, and today we're going to talk about HIPAA and cybersecurity: 5 steps to compliance. And we're going to do it with Bridget Steele. Bridget is an attorney with Barclay Damon, who practices in the Cybersecurity and Health and Human Services Practices. Bridget, welcome to this episode of the Cyber Sip podcast.

[Bridget Steele]: Hi, Kevin. Thanks for having me.

[KS]: Before we get started, I just want to show you I have the official mug of the Cyber Sip podcast. Do you have one as well?

[BS]: I don't have a Barclay Damon mug, but I do have a winter greetings mug with the little snowman on it.

[KS]: So colorful and neutral. So it works on …

[BS]: …in honor of the Cyber Sip podcast.

[KS]: Yes. Well, let's get right to it. We're going to talk about five steps to compliance: HIPAA and cybersecurity, and the first thing we want to talk about is understanding your data and systems. Very important to know what data you have, where it is and who has access to it. So let's talk about that now. What data does an organization have?

[BS]: Yeah. I think for health care providers or organizations working in the health care space, especially, this is really important, you know, understanding, where do you store data, especially health information or sensitive data types, you know, what vendors have access to it, how does that data flow? And I think, you know, if you create sort of an organizational flow chart or, you know, some sort of graphic—especially large organizations and see where data is flowing, and where it's stored and who's responsible for, you know, repositories, it can help identify whether you have any gaps in cybersecurity that you need to address or or tighten up. So that's always a good, a good place to start when you're looking at your cybersecurity. You know things you can do to improve cybersecurity at your organization.

[KS]: Before we move to our next step, Bridget, one of the things I always think about is that there are really two reasons to do this, right? The first reason is at least in the HIPAA context. You are dealing with a heavily regulated industry, and there are laws and regulations with which your organization has to comply. So that's reason number one. But reason number two, I've always felt, is very practical, that if something does go wrong and as one of the guests on our prior podcast said, this is a lottery that you're going to win. You … it's not a question of whether you're going to be breached or have a security incident, it's a question of when. When that does happen, you want to be able to show that you've had a track record of compliance. So very important to be able to say that, yes, we do know what data we have, who has access to it, and for what purpose that data is being used.

[BS]: Mm-hmm.

[KS]: All right. So we talked about understanding your data and systems. Let's say that we we do that and we have created a data flow diagram in order to manage our data. What's the next step for HIPAA and cybersecurity compliance?

[BS]: Well, I think understanding, you know, what rules or laws apply to you. Obviously, HIPAA applies to covered entities which are health plans, clearinghouses, and health care providers that are doing certain covered transactions like billing. It also applies to business associates of covered entities. So if you're a health care provider and you use a health IT vendor that, you know, hosts your data or has access to your protected health information, they are considered a business associate. And they're also required to comply with certain provisions of HIPAA. Most importantly, the security rule obligations, and then you have to have a business associate agreement with them. So those are the two main, you know, categories of parties that have to comply with HIPAA. But beyond that, you know, you also have to look at state laws as well that could apply to you, that govern maybe sensitive types of data that you possess.

[KS]: So I know we're going to talk about business associate agreements in a little bit one of our later steps. But before we move beyond business associates, that's a broad category, at least potentially. Can you give us some examples of business associates that would be covered by HIPAA and its cybersecurity rules?

[BS]: Yeah. So a "business associate" is anyone who could have access to a covered entity's protected health information. So an attorney, a law firm—could be a business associate if you're helping health care providers with you know, billing issues and we have a business associate agreement with some of our provider clients. An accounting firm could be a business associate, vendors, especially, you know, billing companies in … the most high risk, I'd say business associates are those that possess a lot of your PHI. So billing companies, health IT vendors, those types of service providers are our business associates. But you have to really you know, make sure that you're kind of monitoring those. And I think we're going to talk about that at the next step.

[KS]: We are. Let's stay on this step, though, the privacy and security rules, and let's break those down just for our viewers and listeners. Talk about the privacy rule first and some of the key features that every organization should keep in mind.

[BS]: Yeah. So the privacy rule governs uses and disclosures of PHI and whether you need a specific authorization from the patient for that user disclosure. It also talks about certain rights that an individual has under HIPAA. So you know, you have the right to access your protected health information. That's a big kind of initiative going on at HHS right now is if that a provider is not timely providing patient access to their own records, you could be subject to an enforcement action. So the privacy rule is mainly focused on the covered entity themselves, but some of those obligations can be flowed down to a business associate under a business associate agreement.

[KS]: What about the security role, Bridget, and and in particular, how specific is it? Is it sufficient to say that the business associate must, for example, employ "reasonable safeguards" to protect the privacy and security of data? Or does it need to be more detailed than that?

[BS]: The security rule is very detailed, it breaks down safeguards into three buckets, so administrative safeguards, you know, your policies and procedures, having a security officer. Those administrative steps that you take to make sure that you're complying with HIPAA. Then there's physical safeguards which include, you know making sure that physically protected health information is safeguarded, things are locked up. And that type of thing that you're... when you're disposing of PHI, that you're doing it in a way that meets the the HIPAA security rule, you're not just, you know, throwing paper in the dumpster. You'll get an enforcement action for that. And then also technical safeguards that are in place, you know, when you access, when somebody logs in that they're using a certain password, maybe multi-factor authentication that you audit your systems and access that's going on, that you have firewalls in place. So the HIPAA security rule is pretty specific. Some things are addressable, meaning you have to look at whether you need them and then make a determination whether you need to implement a certain safeguard. Or they're required, meaning, you, you have to, you know, meet those certain safeguards and implement them.

[KS]: Can you give us an example of some of the required safeguards?

[BS]: Yeah. So I ... access controls are required. Encryption is actually addressable. But at this point in time, its ...

[KS]: Meaning it's not actually required as we sit here today.

[BS]: But what you have to understand about "addressable" is you can't just, you know, decide, you know kind of arbitrarily whether to implement something. And in today's world, it's really hard not to say that you have to implement encryption. So most organizations need to have encryption implemented, because when you look at the risks and weighing the risks that your organization faces on a day-to-day basis, you really need to be using encryption. When PHI is at rest or in in transit.

[BS]: No, and I think we've seen and been involved in enforcement actions and regulatory investigations. And in our experience, at least it's not a very useful answer when the regulator asks, do you have multi-factor authentication? Do you have encryption or smart passwords? And you say, Well, no, I don't, but it's not technically required by the rule. The regulators like to know that the organizations within their purview are following best practices at this point.

[KS]: Yeah, and I think saying it's not technically required is a little misleading because when you ... if you look at the risks you would in, the only determination you could make is that you need to implement it, then it essentially is a requirement. So.

[KS]: Yes.

[BS]: A little bit of a confusing point, but I think it's an important one.

[KS]: So we talked about understanding data and systems, and we talked about the HIPAA privacy and security rule. Our next step is is vendor management or what I like to call vendor management. But this is really the piece that involves in organizations sitting down with its business associates and developing an agreement that implements, in effect, these safeguards, right?

[BS]: Yeah. So the business associate agreements are have to be in place between the covered entity and their service providers that could have access to PHI. Typically, there's some sort of underlying service provider agreement that might cover limited liability and insurance requirements. Sometimes some requirements are built into the BAA themselves. A lot of the clients we work with these days, their standard BAA form that they use goes way above and beyond what the minimum requirements are under HIPAA. And there's a lot of, you know, requirements. From a security standpoint that are in their BAAs that, you know, are just kind of good practice or best practice you know, if you are a service provider contracting with a hospital, for example, you're going to see provisions in there that are pretty standard, like you can't you know, store data offshore, which means outside of the United States. You know you, you can't sell PHI. You need to have a certain security certification. These types of things that are, you know risk mitigation for the providers when they're working with these vendors to make sure that you know, their data is protected.

[KS]: Now outside the HIPAA context, Bridget, there's a balance that we always struggle with, right? On one hand, as an organization, you're dealing with a vendor. You want to build as many protections into the agreement as you can. But you're always worried that if you overbuild, you're going to scare vendors away, or vendors are going to say, you know, we'd love to work with you, but we just can't comply with these onerous requirements. And then on the flip side, if you are a vendor or a business associate, you're going to want to do everything that you need to comply with the law. But you're going to want to limit those impositions because you want to be careful not to overpromise or not to agree to do things that you can't do. How does that balance play in the HIPAA context where there are these legal requirements? Do health care organizations or vendors struggle with that balance: between the need to comply and the need to be reasonable in terms of what can and can't be done?

[BS]: Yeah, I mean, the balance is exactly right, and there's a little bit of a squeeze going on because, you know, providers are under a lot of pressure or risk or there could be regulatory requirements that that, you know, they have to impose on their downstream vendors. And I think where I see the squeeze a lot is when you have a business associate who works with another downstream vendor—subcontractor—and they have to have a subcontractor business associate agreement in place, and they're trying to flow down the obligations that are upstream with their provider customers down to that downstream vendor, you know, they need it, they need to work with these vendors. And so a lot of times they're, you know, trying to balance the, you know what, we'd like working with these vendors, but our customers are, you know, coming up with more and more difficult and onerous requirements. And there is a little bit of there's always going to be a balance going on but if you... in the health care space, especially, there's a little bit of a mentality that if you're going to play in the sandbox, that you'll meet a lot of the requirements of customers. But of course, there are vendors that have a lot of leverage, too. And so it depends on who you're working with, what their requirements are and whether they... there is the ability to negotiate and it can be different in different scenarios. But there's always that balance going on.

[KS]: Right. And I think in our episode 1 of the Cyber Sip podcast, we talked about the three Cs of cybersecurity for vendor relationships, and I like to think of them as confer—you sit down and have a conversation about these things that we've talked about. What data do you have? Who has access to it? What are the safeguards? Contract—so you're going to build these protections into your agreement. And then comply—you're going to follow up and even audit to make sure that both sides of the relationship are doing what they say they would do. What's your experience on that? Sometimes I think it's just a battle of the forms. One party will send out their version of the contract. The other party gets a lawyer and sends out another version and somehow they come together. But is that really the right way to do it in the HIPAA context?

[BS]: I think it's always best, when you know, the business folks have an understanding at the outset and then, you know, they might bring in their attorneys, which is an important thing to do, especially when you're dealing with an expensive contract where a lot of data could be accessed by a vendor. But when you're an attorney you want to understand the goals of your client. And not just be looking at a contract, and kind of understand the big picture. I think when when things are rushed it's difficult. And you're or when you're in a position where like, we need to sign this contract in two weeks or three weeks. So I like your first "C," which is confer, I think, you said, right?

[KS]: Yes.

[BS]: You know these are...shouldn't be something that's put on the back burner when you have an important, you know, contractual relationship or vendor relationship. You want to kind of get that planning phase started early on so that, you know, you're well positioned, everybody's on the same page; people understand each other's goals so that when you actually go into the contracting process, it's one, not rushed, and two, thoughtful. And then, you know, if it feels fair for both parties, then I think it's going to be a good relationship or partnership moving forward.

[KS]: All right. So we talked a little bit about vendor management. The relationship between the health care provider and the business associate. I want to move on to step four now, which is responding to privacy and security incidents. And I think the first thing that you want to talk about is reporting. So let's say that you have an incident and maybe that's let's set the table Bridget. So give us an example of a more common privacy or security incident that an organization may experience and then walk us through the reporting of that incident to federal and even state authorities.

[BS]: Yes, so a common one could be loss of a laptop or a mobile device that had PHI on it, that wasn't encrypted. You know, they really should be encrypted, especially if you're, you know, working from home or you know, using it a lot and moving around. So if PHI is on any of these devices unencrypted and stolen or lost, that's common. Another common one would be that we've seen is somebody leaves an organization and their access to certain repositories isn't terminated. And maybe they go to a competitor and they login or something like that. So if there is a breach and it impacts more than 500 individuals ... meaning there's PHI of more than 500. Individuals and...

[KS]: Sorry to interrupt. But I just want to make sure I'm sure we all, or many of us know what it is, but when you say "PHI," you mean "personal health information," can you give us an example or two? It's... I know it sounds obvious, but what types of information are we talking about?

[BS]: Yeah. So it's PHI is actually a fairly simple... the simplest way to think of it, and I'm kind of boiling it down a little bit is "identifiable health information." So something could be PHI if it is an agency that you receive services at, "Kevin Szczepanski" at a certain health care provider receiving services... that's PHI because your name, Kevin Szczepanski, along with the fact that you receive services at a certain agency those two together would be PHI, so it can be pretty easy if you're storing PHI, you know, especially if you are on your mobile device or on your laptop, if you have any kind of billing files or spreadsheets with patient-specific information and you lose that laptop or mobile device, you know, you're in a breach situation and you have to presume that you have a breach unless you can do a risk assessment and determine that there's a low likelihood that that breach occurred.

[KS]: All right. So let's talk about that because I think that's an area that is confusing and sometimes even frustrating to those who work in the industry. Let's say that you find that you left your laptop in the car overnight. You wake up in the morning to find that it's been stolen. And fortunately, a couple of days later, you get a call from the local supermarket and they say, Hey, I found your I think I found what's your laptop. You go pick it up. You've got it back. It's workable. How do you decide, then, that the information has been accessed, triggering a reporting obligation when you're not sure? And in fact, it might very well be doubtful that someone... random person broke into your car for the purpose of accessing someone else's PHI. How does that work?

[BS]: Yeah, you'd have to do a risk assessment. You know, in that situation, you may bring in someone to do a forensic review of the laptop. You know, was it turned on during the period that it was missing? Is there any way to see whether anything was accessed? If you can, you know if a forensic review can show that it wasn't you know, turned on or accessed during a specific period, then you may be able to reach a conclusion that you don't have a breach. I think a lot of times and a lot of areas where we deal with in the Cyber group is when you don't know. And a lot of time, typically when you don't know, it's hard to, you know, overcome that presumption that you have a breach. And you mean it may be reportable, but you have to look at different factors. You know, if it was left … if you work for a health care provider and you went to a hospital and was left with a hospital. And then they returned it, it may not be a breach because you're both covered entities. And, you know, if they sign something saying nobody, you know, nothing happened and we kept it secure, whatever you might be able to to reach a determination that there's not a breach, but it's very case specific. It's very fact heavy. And you also have to produce a written report so you can't just say, you know, subjectively make a subjective determination. And and, you know, say and not a breach and go on. You have to look at the factors, weigh them and you have to have a written analysis that you keep in your file.

[KS]: And that written analysis comes at least first from the forensic provider, which to me underscores the need to retain a capable, experienced forensic effort expert who can look into the matter and tell you whether or not the areas in your system containing PHI were accessed. If not, then you may be able to call it a day, but if that access… what happens, if that access can't be ruled out? In other words, there's no evidence that a bad actor did access PHI, but it's theoretically possible, and the forensic expert can't rule it out.

[BS]: Yeah.

[KS]: So in that case, I guess, the tie goes to the runner, in other words, if there's any doubt that creates a duty on the part of the provider to report it to the appropriate authorities.

[BS]: Typically, like I said, every situation you have to look at all the all the circumstances. But yeah, in the example you described. We left it Tops or any grocery store or something that would generally be a be a breach, if you can overcome that presumption.

[KS]: So let's follow that scenario, and because I know you've dealt with these situations, let's suppose that you can't rule out a breach that … and the computer of the affected computer or laptop did contain PHI and it had the PHI of more than 500 individuals. Walk us through the significance of that and in particular the significance of the number of individuals whose data might have been accessed.

[BS]: Yeah. So if you work for a business associate, you'd have to look at your BAA because you may be obligated to report up to your to the covered entity or covered entities whose information you have stored on that. But if we're looking at a provider, for example, a covered entity provider, they would be required to notify the individual affected. They'd also be required to notify HHS, OCR if it's less than…

[KS]: Walk us through that. Health and Human Services…?

BS: Yes

[KS]: OCR?

[BS]: Office of Civil Rights, it's within HHS. So you'd have to notify HHS through their breach portal. And you typically want to, you know, you obviously have to get your arms around the scope of the breach before you do the reporting, which a lot of times involves a forensic analysis that can take time. But you you have 60 days to report. And then you also in New York state, have to report to the Attorney General's office five days after you report to HHS. And then if there's a breach of private information which could include like Social Security numbers, that's separately regulated by the attorney general and you'd have to report to the attorney general on that as well. You also may want to look at some of your contracts, especially if you're a business associate or service provider, to see if you have reporting obligations to your customers. You know, we've been seeing lately that there are customers that just want to know if you have a breach, even if it doesn't impact their data and they have really, really strict requirements in their contracts, saying, hey, if you have a breach you have to tell us, even if it's a breach of your systems, it doesn't involve our data. So I think there's a lot to consider. And, you know, it's kind of an all hands on deck situation when you have a major breach of more than, you know, a certain number of individuals impacted.

[KS]: Yeah. Sorry to interrupt. Two quick points, though I wanted to underscore, is that if you do have a HIPAA breach, it doesn't mean that you don't also have to report the breach under applicable state law, right? So you can have you could have a double set of reporting requirements.

[BS]: In fact, yeah, under the SHIELD Act [Note: Stop Hacks and Improve Electronic Data Security], which came into play a couple of years ago in New York...

[KS]: The New York SHIELD Act. Yes.

[BS]: You have to report within that five-day period. Even if it's not a breach of private information. So if you have a reportable breach to HHS, you have to report to the attorney general. And the reason for that is, the attorney general can independently enforce HIPAA. They're sort of like the new sheriff in town, and we've seen the attorney general doing more HIPAA enforcement over the past few years.

[KS]: And this is to me, Bridget, kind of where the rubber meets the road. So we've talked about data classification, implementing the HIPAA privacy and security rules, vendor management. Now, if you do have if you do happen to have a privacy or security incident that becomes reportable, you may find yourself with one or two federal and state and possibly multiple state regulators, depending on where your consumers, or your customers reside, conducting investigations and asking you the very questions that we've been talking about. Well, where is your data? Who has access to it? Give us an explanation of how you've complied with the privacy and security rules. Let's see an example of your business associate agreements. How have you been enforcing those rules across the spectrum with your vendors? And so if you haven't taken all the steps that we've talked about thus far, it can be a more uncomfortable regulatory investigation than it needs to be, right?

[BS]: Oh, yes, certainly. I mean, and that's a lot of times where a provider will get get hit is is there is some sort of breach and there is an inquiry or a request for information and, you know your answers kind of indicate that, you know, you really haven't been complying with HIPAA before this breach happened, maybe you didn't do a risk analysis, looking at ... which is required under HIPAA, which is essentially, you know, looking at where you store data and where you have gaps and trying to kind of shore that up. Maybe you don't have adequate policies and procedures. Maybe you're not training your your workforce appropriately on HIPAA. So, yeah, you want to make sure that, you know, because I think we both know that you can be a perfect you know, HIPAA-compliant entity and you can still suffer a breach, you know, or an attack. So you want to be in a position where you can say, look, we've done everything we could. And this still happened and we're going to continue to take measures to make sure something like this doesn't happen again.

[KS]: And as we've seen in the regulatory investigations, we've been involved and it can be much easier. It's not not that it isn't challenging, but it can be much more effective if you can tell that story of compliance.

[BS]: Right.

[KS]: And of course, we've we've seen occasionally we've seen situations where that can't be done and every situation is different. Sometimes we can help in those situations, too, but it is much more challenging if you don't have that record of compliance to talk about it...

[BS]: Right.

[KS]: So in the time we have left Bridget, I want to talk about the fifth step of HIPAA and cybersecurity, that fifth compliance step and that is, learn from your mistakes, right? So talk about that for us. What what mistakes and how do we go about learning from them?

[BS]: Yeah. So I think I talked about some of the common calls that we get you know, from our health care clients, there is there's missing, you know your laptop lost or lost phone, misfired emails, misdirected mailing, you know, when you terminate someone and you don't terminate their their access controls or access rights to certain databases. So those are our common calls, but you have to kind of... when you have issues or reports, you have to shore up, you know, what you're doing and how can we improve on what we're doing? So looking at your policies or improvements to your policies, you know, following along with what what's going on. In terms of enforcement, doing audits and always looking to get better...

[KS]: Bridget, can I step back for a second? You mentioned following along in and looking at enforcement actions. Talk to us about how an organization can go about doing that. Because there are online sources that we can track, that a business can track to see what's going on in the field and learn from those experiences that others have had.

[BS]: Yeah, I'm... HHS issues, press releases, where they talk about, you know, ongoing settlements or investigations that were resolved. And you can go on HHS's website and look at that. HHS also puts out guidance documents, I mean, you can follow along with our health care group issues, you know, email alerts when there's something that might come out and we we do webinars and we provide trainings too, to staff and to boards of directors on HIPAA compliance. But, you know, you just looking at common threads and even being involved in provider groups or associations. Those are huge sources of information...

[KS]: Absolutely.

[BS]: To keep you in the loop. But really just kind of having your ears open. And you know, like I said earlier, one of the biggest enforcement trends that are coming out of HHS is right of access. So making sure that patients can access in their personal represent... representatives can access their own health records. That's a huge thing right now. So now would be a good time to look at that issue if you feel like there are gaps and in, you know, responding to requests for records.

[KS]: One other thought I want to get your thoughts on before we close and that is the remote work trend really the the mandatory remote work trend. How has that affected cybersecurity compliance in the HIPAA context?

[BS]: Yeah, I mean, that's, you know, more and more people are doing work from home and, you know, you can't forget what you've learned in your your HIPAA training. So, you know, if you have paper records at your house, you can't throw them in your garbage, you've got to make sure you, you know, shred them in a HIPAA-compliant way. And typically probably means bringing them back to your office but you know, following the guidance that your job requires of you and HIPAA training requires of you: making sure that you're using a secure connection. You know, don't let your, you know, everybody in your family use your computer if you have PHI on it that's not good. That's, you know, a potential HIPAA violation. So just because you're working from home, you can't forget about, you know, all of the requirements that you have under under HIPAA. And you really need to be looking to your organization to give you guidance on on what is appropriate and what's not.

[KS]: Right. Well, there is so much more to talk about and we can't talk about it all today. But will you come back and talk to us again about remote access and HIPAA compliance?

[BS]: Sure. I'll bring a different mug next time.

[KS]: All right. I will, too. Thank you for coming and talking to us a little bit about HIPAA and cybersecurity: five steps to compliance. I've enjoyed having you on and look forward to you coming back some time.

[BS]: My pleasure. Thanks, Kevin.

[KS]: And and thanks to all of you for watching and listening. We'll see you next time.

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

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