Healthcare Regulatory Roundup #89 Webinar Transcript

Proposed Changes to the HIPAA Security Rule – Speak Now or Forever Hold Your Peace

Presented January 26, 2025

https://www.pyapc.com/insights/on-demand-webinar-proposed-changes-to-the-hipaa-security-rule-speak-now-or-forever-hold-your-peace/

Please note, this transcript was generated automatically. PYA cannot guarantee its accuracy or completeness.

SPEAKERS

Barry Mathis, Erin Walker, PYA Moderator

SUMMARY KEYWORDS

HIPAA Security Rule, proposed changes, ePHI, cybersecurity, data encryption, security risk analysis, documentation, incident response plan, vendor management, compliance audit, audit reporting, training, access controls, network monitoring, data encryption, breach notification, business associate agreements, continuous process

WEBINAR SUMMARY

The webinar discussed proposed changes to the HIPAA Security Rule, emphasizing the need for enhanced cybersecurity measures. Key points included the shift from addressable to required encryption, the need for clear documentation, and the importance of comprehensive risk assessments. The proposed rule aims to reduce ambiguity and enhance preparedness, with a six-month grace period after publication. Specific requirements include detailed incident response plans, regular testing, and thorough vendor risk assessments. The webinar also highlighted the importance of continuous training, proactive monitoring, and executive involvement in compliance efforts.

The webinar focused on 5 key topics:

1. Introduction and overview of the proposed changes to the HIPAA Security Rule
2. Impact of proposed rule changes
3. Compliance implications and preparedness
4. Strategies for preparedness
5. Final thoughts and next steps – preparing and continuing education

ACTION ITEMS

- ☐ Review the proposed rule changes and provide feedback/comments by March 7, 2023.
- ☐ Assess the organization's current security risk assessment process and documentation to identify gaps that need to be addressed.

- ☐ Evaluate the organization's current data encryption practices and develop a plan to implement robust encryption across all systems handling ePHI.
- ☐ Review and update the organization's incident response plan to ensure detailed procedures are in place, including regular testing.
- ☐ Conduct a thorough risk assessment of all third-party vendors and business associates that handle ePHI, and update contracts as needed.
- ☐ Review and update access control policies and procedures to ensure appropriate role-based access, timely termination of access, and comprehensive logging and monitoring.

TRANSCRIPT

PYA Moderator **00:06**

Thank you for joining us. The webinar will begin shortly.

Good morning, everyone. Welcome to the latest episode of PYA is Healthcare Regulatory Roundup webinar series. Today's topic is *Proposed Changes to the HIPAA Security Rule – Speak Now or Forever Hold Your Peace*. PYA is happy to present today's webinar on this important topic.

You may submit questions during the webinar by typing a message into the Q&A pane of the control panel. Also immediately following the end of the webinar, you'll be asked to complete a short survey and submit any additional comments and questions. Any questions posed during the webinar will be responded to via email after the webinar. We've posted a PDF copy of the presentation slides for your reference in the Resources pane. You can also customize your viewing experience by resizing, moving, or minimizing all of the panes within the webinar.net. platform. You'll receive an email later today with a copy of the slides and a recording of the webinar.

With that, I'd like to introduce our presenters, Barry Mathis and Erin Walker.

Barry Mathis **01:34**

Hello, everyone. My name is Barry Mathis. I'm a principal with PYA, leader of Information Technology Advisory and Consulting. You'll notice on your screen my colleague, Erin, appears to be frozen. I literally just got a text that said her power it went out in her grid. So, we had planned for Erin to take the first portion of this, and I would do the second, so I'm going to start in Erin's. Covering for her, as we often do for our colleagues, things are not perfect, but you know, as Steve Jobs once said, if you know what you're talking about, you really don't need the PowerPoint anyway.

But we're going to talk about for a little bit the proposed changes. It's all the buzz right now, a letter from the several different organizations, not calling out any organizations, a lot of people putting comments in on the proposed changes to the HIPAA. And we're talking about security, designed to enhance the cybersecurity. There's a lot of people who don't think the changes are really going to do that, and you may have an opinion on that. We're going to talk about how you may provide your comments as well, and we'll talk about the comment period, which ends, I believe, March the seventh. But we're going to talk about what they are. And again, this is not intended to be a certifying class. In in all the proposed changes, it's we only have an hour, and we're going to cover the key points and the finer pieces.

The one thing I'll just tell you up front that we're not going to look at is we're not going to go into a lot of the exceptions, okay? But there for all of these proposals, especially around encryption, there's, there are some exceptions, but we're going to tell you basically what the things are saying. And then I'm going to go into a couple of more points on the impact, both positive and negative, and depending on your situation, small hospital, single practice, large ID or academic medical center, these may all resonate differently with you. So, I'm going to try to cover the different areas, and then strategies to prepare.

There's some companion articles, if you go to PYA Insights – hit our website, go to PYA Insights – there's some companion articles on the outlines these. And then even a nice kind of tongue-in-cheek about getting prepared for that New Year's resolution and losing weight and getting fit, how you might use that kind of thought pattern to help prepare for some of the HIPAA changes that may be coming or that are likely coming down the pipe. So, I'm going to jump right into it, overview of the proposed rule changes.

Okay, uniform implementation simplifications, one of the biggest things you're going to write off. And for those of us who have been doing, you know, the HIPAA assessments, like myself, for, you know, 20 plus years, it's or nearly 20 years, 96 and then four, they're a little bit of ambiguity on addressable and required. I'll give you one example. Did you know that under the letter of the current rule, encryption is actually an addressable item? Now you're going to have a hard time explaining an investigation why you chose not to encrypt it, and there's guidance that have come out from HHS and OCR on what you should be doing with encryption, but you're not going to win the argument that says we're going to run a car into a wall. Maybe we wear a seat belt, maybe we don't? Let me help that argument. No, it's absolutely something that makes sense to do, and you should do it, and the guidance tells you should do it. They're getting rid of that, these things are important. Especially around the security pieces, they're just going to make them required. Now we're going to talk positives and negatives about that, but just know that ambiguity is going to go away.

Documentation. If you've ever done, if you're a professional services firm like PYA and you've worked with a client on doing an assessment, one of the things that we issue is a request for information. And what we're trying to do is glean, based on what we understand, is what you're going to need to provide as evidence of controls. All of these documentations, and it is a kaleidoscope for us, as it is for the federal government. Likely, when they're doing their audits based on some kind of a breach, a report, or corrective action plan, or CID, absolutely all over the place. You ask 10 different people what a risk analysis is supposed to look like, or what the artifact should be, and you're going to get 12 answers. Okay, they want to cut down on that, so there's going to be. Personally, do I think they've gone far enough? Maybe not, but they're going to help try to narrow down what specifically that documentation needs to be, and then label some very specific things like incidence responses and network configurations. Again, kaleidoscope.

When Steven Lennon, who's our CIO, who helps me on a lot of stuff, I really appreciate Stephen and his team. When we ask for a network diagram or topology for an assessment we're doing, we don't know what we're going to get. Sometimes we can read it and understand it. And in the past, there is a thought that who you're sharing it with in terms of the other side of the audit may or may not understand topology. Anyway, my belief in understanding for these changes that are happening is that person reading that's going to understand it. They're going to give you some very specific standard. Look, we want to see a true network diagram, topology. We want to know that you know where your universe is, and that's common with documentation, policy, procedures, networking. The federal government wants to know, do you even know for 100% sure what your environment is, all the pieces to it, when it relates to what may be,

connecting, touching, sending, receiving, storing, backing up, all this kind of stuff, ePHI or PHI? Along with that, the asset inventory network. I touched on the network a little bit, but we could say the same thing for asset inventories. When we ask for, do you have an asset inventory? 80% of the time we get essentially something that comes from an online tour that comes with the OES, the Original Equipment Service provider, what's on the wire, right? So, we can see all the network things on the wire right. Clip run the report, we can see that it's going to go beyond that, right? What's on the shelf, what's sitting to be decommissioned. Do you know the disposition of that? Can you accurately say all the devices? Okay?

Now, to make this almost impossible, let's throw in Internet of Things. And remember, if you don't know what IoT or Internet of Things is, it's all the other things in your house. That fits that category. Now, obviously the rules for us in business, to describe Internet of Things, it's that picture frame that has a wi-fi on it, that touches it. It's the coffee maker. It's the refrigerator. If you've got one of them fancy refrigerators that tells you, go away, you've been here three times, we haven't grown any food, there's nothing to eat, go the grocery store. All of those things, if it touches the internet, if it shares information, it's part of the Internet of Things. Within a healthcare organization, there's a lot of that stuff. And if I paused and said, right now, we give everybody three minutes, okay? And you think about, do you know where all of those devices are in your organization and whether they do not touch something that either stores, sends, receives ePHI? I'm betting in that three minutes we get a lot of frustrated people saying, I don't think so. You're going to want to, that's going to be part of that asset inventory. Going forward, you're going to have to be able to show, at least as the way the proposed rule is now, a lot of comments out there on the possibility of some of that and maybe there's a longer time frame to get there, but right now you're going to have to have that if it passes the way it is.

Enhanced risk analysis, again, this goes back to giving some directions on what is supposed to be in the risk analysis, and this may be an area where I think they could probably, you know my opinion personally, provide some more guidance in this, as opposed to less. Because there's already guidance for how to conduct a security risk analysis, okay? And they use, if you're not aware of there's a clear guidance from HHS on following NIST, or the National Institute of Standards and Technology, which was born out of the federal government to build airplanes, tanks, bullets, and band aids. They use that, and with that is a massive, massive framework, guidance documentation. Within that they have called special publications, and within the special publications there's an 800 series around security and privacy of things. And there's one called SP 30, and that is what they're saying, is that's what you should be following to do your secure risk analysis. Likely that's going to hold, but they may get more granular, because that's not in if you go back and read, you know, CFR 164 308, right? You're not going to see a reference to that. The guidance has come out after that. Well, likely the new rule is going to actually be thrown out, instead of guidance it is going to be requirement, right? So, get rid of ambiguity. Here's what we expect. And also, they can say, look, it may be that you can't do it internally, right? There's discussion out there with some of the language that's really kind of a third-party. We think a third-party, independent review, is the thing you should be doing anyway. There's guidance for that, but it may be a required thing.

Access to termination notifications. So, we're very good as an industry, or we're better than we were years ago, on provisioning the person entering our organization should he or she have access to certain data applications? But we have been less successful as an industry, and when that person leaves, okay, making sure those credentials are suspended for access. Because sometimes you can't remove the credentials because it's the ID is attached to documentation and EMR, but certainly you want to make it so that person can't reuse those from the outside, or even from the inside. We're not as good as an industry with that, and

I'm not picking anybody in particular, as an industry as a whole we've not been great. Well, they're raising that bar, right? Because notifying the members within 24 hours of termination to access ePHI, you got to let them know it's gone, and the only way you can let them know is if you're doing it. So, it's kind of a way to get this side moving there to get it done.

And then, I'll go ahead and do the final couple of bullets on this, and I'm..look, Erin's back. Erin's got her power back, and she's back. I'll look at her here. It looks great, Erin. I'm going to do the last couple of bullets on this, and then I'm going to turn it over to you. Okay? Because I want folks to hear from you, because you are in the middle of this with us and have a lot of good things to say. I'm just going to carry the water while you got that power going back. And so, the hamsters are running, Erin's got lights, and we're going to move on.

Contingency planning and incidents response. This is a, there's a lot of discussion, you know, as they were going through these particular concerns. Obviously elevated because of cyber-ransomware and everything that's happening. What they were discovering, when I say they, it's pretty much through this conversation going to be OCR, HHS, OIG, others in that in that sector, primarily OCR and HHS. They were seeing as part of their investigations, again, a kaleidoscope of efforts and in some cases, a black hole where there should be a clearly defined, with clear roles and responsibilities, and activity, and testing an incidence response plan. And I would guess all of us have asked in our assessments, and likely you've been asking your assessments. And here's the challenge that I would give to you: go look at one of your previous security risk analyses that you had done, and you should be able to go back, because in a Federal Audit, you're going to have to six or seven years. See if on there they mentioned what's known as a business impact analysis disaster recovery and contingency and see how long that can has been kicked down the road in your own organization. By the way, Office of Civil Rights, Health and Human Services, they would call that “systemic noncompliance”. Well, they're raising the bar. They're going to make it very plain what you should and shouldn't or have, and have to do, but they're expecting that comprehensive Incident Security Response Plan and a comprehensive business contingency. Now the thing that's getting the most comments is that 72 hours. 72 hours, I don't typically read slides, but I'm going to read that sentence, okay, establish procedures. Again, establish the procedures to restore lost systems and data within 72 hours. Not going to happen. I mean, I don't know who you're going to hire. I don't know what vendor you're using that if it gets completely ransom, that you can respond every piece of it. So, maybe some additional language there. Maybe in 72 hours you need to be able to treat a patient based on the information that was there something. But just blankly saying, we need systems up in 72 hours. Wow, what a check that's going to take to write.

And then finally, annual compliance audits and business associate verification. The BAs have been there for a while. I. There is now within this language, probably the thing that gets my attention the most is that they're looking for us and you to also be accountable and responsible for the BAs of our BAs, right? So, it all comes into third-party vendors. So, we can put that all in a bucket of upstream, downstream, third-party, vendor management. There's a lot of focus on that. I encourage you to go look at some of the exceptions there and provide comments if you want to provide comments to the federal government by the seventh, but that's a that's another big lift for us. Okay, Erin, I'm going to, if you want to take control, I'm going to give that back to you and let you carry on, ma'am.

Erin Walker **15:47**

Okay, so, let's talk about that for just a quick second, a little bit more. So, there is, as Barry mentioned, a public comment period. It is open for 60 days. This is a really important opportunity for you all, for organizations, for any anyone, any stakeholders in your organization, to provide feedback on these proposed changes. Like Barry was just referencing, it's a really important step in this process before the rule is finalized and implemented, because it allows the government to review the comments and take them into consideration. As noted here, the comments have to be submitted by March 7, 2025. HHS will review those, but we would really encourage you to provide your feedback and make comments, because these proposed updates are they bring a lot of work that's going to have to be done in order to comply, and the timelines for compliance are enhanced. They're increased, as well as accelerated timelines for the updates themselves. So, we would really encourage you all to go and make these, go and provide feedback, make comments, and just do so by March 7.

Now, once the final rule is published. So, right now, it's proposed updates. Once the rule is published, there will be a six-month grace period after the rule is issued to implement the necessary changes. And based on what Barry just described as regarding the updates, there's a lot of changes that are going to have to be implemented. So, six months is a short time frame window, and so it's really important now that everyone be aware of what those proposed updates state, and really look at your organizations to determine what would it take for us to be able to comply?

During the grace period, the HHS is expected to offer some guidance on compliance and implementation. But again, it's a six-month period, and after that period ends, after that six months, enforcement will begin. And HHS will be conducting audits. They'll be conducting investigations to assess compliance with the with the updates, so not just audits of where you were before, but where you are now, after that six-month grace period ends. We've provided here a couple resources for you. I know that you all are going to get copies of the slides. These links will take you to a couple articles regarding a summary of the proposed rule, what the updates entail, and also, what are the compliance implications. What should you be looking at? We've heard about the updates. We know what they say. We know what they say the expectations are, but, but what does that look like from a compliance perspective and an implementation perspective? So, we would recommend that you go take a look at these articles, and again, they're hyperlinked here, and they'll take you directly to the article.

Now that we've gone over what the updates are, what the proposed updates are, we wanted to take a few minutes and talk about, what are the compliance implications? And when we talk about compliance implications, it's really about, what should you be looking at to see if you have ready? That either you have it already or you know that you're going to have to add it to a work plan so you can get it developed, reviewed, approved, and implemented before the final rule goes into effect.

First, security risk assessments. The security risk assessment process is the updates are going to require more comprehensive and frequent risk assessments. This is no longer an annual thing. This is no longer something that you do every now and then. This is an ongoing process. So, as part of looking at the compliance implications that come with that, how do we implement this? How do we ensure that we're doing, that we're working through an ongoing process and that we're continually updating? It's a live, breathing document, the risk assessment itself. So, you know, assessing not only in your internal security controls, they're going to require that you're evaluating those risks with those third-party vendors that

Barry talked about, with your business associates, even with other healthcare organizations, for example, that you do business with and transmit data to and from. The updated requirements will also require detailed documentation of these risk analyses. So, what are your methodologies? What are the findings? And what are the actions taking taken? So, it's no longer just do a risk assessment, get some findings and work towards them as you can. It's going to be, what are the actions you're taking? Have you reviewed these internally? Have you developed an action plan and are you working towards mitigation? I would point out that this documentation is key to the risk assessment process, following all the way through to those recommended corrective actions and mitigation strategies, because it will be key during an audit. So, if HHS OCR comes in and does an audit, they're going to want to see the documentation, and it will extend far past just we did one last year. They're going to want to see ongoing assessments of the security risks within your organization, both from your organizational standpoint, just as you as an organization, but also from what's occurring in the industry, from what the emerging cybersecurity risks are out there, they're going to see that you're looking at those on a continuous, continual basis.

So, data encryption. The updates are going to require encryption at the end of the day, it was addressable. If the proposed rule gets approved and gets passed, the updated or the addressable versus required specifications are going to go away. So, while encryption was technically addressable, it's going to be required. And this will include all systems that handle ePHI. It will include networks, devices, cloud services, and you're going to have to show through documentation and evidence that robust encryption technologies have been implemented to safeguard the data that are included in all of those systems. Compliance will require encryption software and hardware, but also regular updates and audits that you're able to document and show what you're doing to ensure that encryption protocols that you've implemented as an organization are remaining current, and that they're being updated in response to emerging threats. So, things that we're seeing in the industry, trends that we're seeing, are you updating your encryption methodologies in accordance with what's being seen? So, with regard to data encryption, I would just say that, where are you with that? And what systems do you have that aren't encrypted? What devices do you have that aren't encrypted? Because not only is it going to be required, but you're going to have to be able to evidence and document that you have robust methodologies in place.

As it relates to incident response and reporting, again, detailed incident response plan. Do those plans provide detailed procedures for how you identify, contain and mitigate any potential or actual security incidents that are related to electronic protected health information. What do your procedures look like for breach notification in a timely fashion, and as we'll hear and we have heard, those reporting requirements are going to be accelerated. So, what are the procedures for that? How are you ensuring that effective individuals, regulators, relevant parties, including the media, are informed with regard to or within those established timeframes? How are you doing that? What are their procedures? And do you have a good, documented plan that everyone could follow, that everyone could understand, and have you done training on that? You will also be required to document evidence of regular testing of that incident response plan. They want to make sure that you're able to show that you're testing it. You've looked at every scenario you can think of. You're testing that incident response plan against those scenarios, and that you're as prepared as you can be. We understand that there's going to be things that happen, that that maybe you might not think about. But what are you doing with regard to testing those plans? I can't tell you how many times we'll be speaking with clients or working with clients, and they have a great plan, but they're not testing it. And so, if they're not testing it, how are they ensuring that it's appropriate and will be effective?

With regard to vendor and third-party risk as it relates to compliance implications, thorough risk assessments of all third-party vendors and your business associates that handle electronic protected health information. And when we say thorough risk assessments, it's not just filling out the BAA. You need to be able to document that you're ensuring that they're meeting the security standards that are outlined in the Security Rule, and that includes the updates that we're waiting on. You know, how are you ensuring that? How are you following up with them to make sure that they're keeping any data of yours safe and protected, in compliance with that security rule? And can you evidence that you're doing that? So things to think about are evaluating security measures, data protection policies, practices, risk management frameworks that those third-party vendors are doing. Are they doing a risk assessment? Do they know where their risks are? And if they do, what are they doing to mitigate those and lessen the risk that they've identified? But also ensuring that your contracts with these parties, these third-party vendors, these business associates, have clear provisions for compliance with the HIPAA requirements. Do they? You know, take a look at your contracts, what do they say right now, and looking at them and what they say right now, and looking against what these proposed updates are for the Security Rule, what edits need to be made? What revisions need to be made, and are you prepared? Are you working towards getting those made so that you can ensure that your vendors are remaining compliant and have appropriate documentation? Also, with regard to that documentation, does it include the verification of the fact that the vendors have appropriate safeguards in place? I can't tell you how many times when we're working through an incident response or we're talking with clients, it does involve their third-party vendors. We're having to use them more and more just to continue to provide streamlined healthcare and get the technology that we need to provide good quality patient care. And so, as part of that, what are you doing to ensure that those vendors have all of those appropriate safeguards in place, and that they're operating effectively ss part of this process? And we've noted it here, training, training, training. So, not only documentation, it's going to be, are you training internally on how we're going to do this process? Once you've developed the process and you've implemented the process, it's going to be paramount that you work to train your workforce, and train those working with those vendors and establishing those third-party relationships, so that you can make sure that this process is followed as part of that vendor relationship.

With regard to access controls, from a compliance implication perspective, how are you documenting the access controls? You're going to have to adjust your access control policies to reflect processes that ensure that only authorized individuals can access sensitive data. Now, I know right now you have to have those, making sure that it's minimum necessary, that it's role-based. But this also includes implementing stronger authentication methods, such as multi factor authentication, establishing those role-based access controls. You may have them in practice, but what are they documented? Could you repeat them? How are you ensuring that that role-based access is actually role-based and appropriate? As well as making sure that you're limiting access to ePHI just based on that individual's need to know? Minimum necessary, again, role-based need to know.

On top of all of that, which we already know we're supposed to be doing and that we need to have in place, user access with regard to when an employee changes roles, leaves the organization, doesn't need the access anymore. Maybe they change a role, and they no longer need access to a system. But it's what are your processes to making sure that all individuals within your organizations have the appropriate access and that as things change so their roles or they leave the organization, that that access is appropriately modified so that it reflects a true role-based access for that individual. The updates also are going to require clear protocols, documented protocols, for terminating access and notifying anybody affected by that. So

even your third-party vendors, if someone's terminating access, who? How are you notifying everyone that works with them? How are you notifying even third-party vendors about, you know, this individual is no longer with our organization, they no longer need access. You're going to have to update and document clear procedures for that. So, where are you again? Take a look at your access control policies. What did those look like, not only for provisioning, but deprovisioning? As part of these update requirements, you'll be needing to maintain detailed logging and monitoring of access events. We do talk with a lot of clients, sometimes EMR access monitoring is reactive, or, you know, it kind of access monitoring is reactive, in response to a complaint or a concern or just something that that doesn't seem right. It's going to need to be proactive. What processes do you have? What systems do you have that can do that for you? Do you have any and not only do it for you, but who's going to be responsible for reviewing regularly those logs and ensuring that access is appropriate.

With regard to audit logs and monitoring, I know I just touched on it a little bit, but you're going to need comprehensive audit logging systems to track all access to and interactions with electronic protected health information. This includes things like user activity, what data they retrieve, they look at, as well as what data they modify, and when they modify it, and what modifications they made. Your logs will need to capture information such as time stamps, identity timestamps, the actions performed that I just mentioned, but also that any unauthorized access or suspicious activity that's identified as part of those log reviews is not only identified, but investigated and mitigated, and corrected appropriately. And so that should all be in these logs, so what do your logs look like right now? You know what are you doing with regard to audit, logging, and monitoring?

Policies and procedures, they're the cornerstone. I love some policies and procedures. But really, the proposed updates are really placing a strong emphasis on development, implementation, and documentation of comprehensive policies and procedures. With these updates, your policies and procedures will need to be updated. So, just want to point that out to you all that you really need to take a look at where you're at now and determine, based on these updates what that's going to look like in terms of updates and revisions.

For reporting, I would just advise you all you're going to have, so that the timelines for reporting are enhancing. They're being escalated. What are your processes now? And how do you need to revise those processes so that you can ensure that you're able to report within the new timeframes?

Breach notification. Under the proposed rule, so, once it goes into effect, you will be required to notify affected individuals of a breach involving ePHI within 30 days of discovery. HHS will need to be notified within 60 days, as well as you know, media notifications if it involves a breach of 500 or more individuals. So, again, really important to look at your breach notification policies and procedures. What does the process look like now? What may or may not need to be adjusted so that that you can meet those deadlines from the proposed rule? Your business associate agreements are going to need to be amended. There's obviously restrictive requirements, for covered entities for example. It's the same for business associates. So, you're going to need to review your business associate agreements and determine what updates need to be made so that you can comply with the updated requirements. Not only you comply, but so they comply. Because if we don't update those, then they're still being held to the current, but once the rules in effect the old standard.

And then I would finally just say that under the updated rule, you'll need to really look at your processes for proactively identifying emerging threats and vulnerabilities. So, what are you doing now? And if you're doing regular vulnerability scans, pen testing, are you looking at those reports and then working to mitigate and develop work plans to correct those deficiencies? Or is it something that that routinely happens, but there's not a lot of review going into it on the backend? There's going to be a lot more stricter requirements for emerging threats and vulnerability management, and so I would recommend that you look at those practices and see what, if anything, needs to be enhanced. It probably will need to be enhanced, but so that you can be prepared to implement those processes and move forward with the proposed updates. So, Barry, I think, oh there you go.

Barry Mathis **34:22**

Very good. Thank you, Erin. Again, Erin Walker, she's one of our superstar managers, and she helps us both in the compliance space, privacy, as well as the security space. We really appreciate Erin today. Sorry you had the hiccup in the beginning, but it was great at I loved it. Thank you very much for taking us a little further into the weeds.

Again, folks, this is not meant to be a master's course and there's certainly not going to be a certification after this. But you're likely going to do some additional education, and I'd be interested if you're interested in learning more about the exceptions, because there are some exceptions to some of these. Some of them have been out there for a while, and some we could likely help you with in advisory nature. Some of them, if you want to know, "Hey, Barry, I want an exception to do a thorough, accurate risk analysis." Probably not the right firm to help you with that, but I can advise you through why it's important. But certainly, "Hey, Barry, with some of the requirements around encryption and access that's requiring MFA, we've got two dozen legacy systems that don't have the ability to do MFA. Is there advice there around how do you how do you get through that and still be compliant? Is there a way to do it? How do you document it? How do you focus on the compensating controls?" So, with every section, there are some exceptions related to those, and some of them have been with us for a while. So, some of this is not new what you're going to look at.

So, we've kind of been doing this in the privacy space for a while, but it is new that before all of these rule updates or proposed rule updates, it was all guidance. In other words, there was ambiguity in the rule, and you could be argued either way when? Well, some of this is just making it clear. It's not. It's not necessarily inventing something that's brand new. It's all designed to help raise the bar on specifics around cybersecurity. That's kind of where it all got started, right? But if you need help with compliance as well as the security, Erin's a great person to get a hold of. We are so proud to have her on our team. Erin, thank you so much.

We're going to jump in. So, besides the implications, each of these implications have some impacts. I'm going to go over four, and they're arguable. I get it, depending on your situation and where you're at, you may say, well, Barry, I think that positive is a negative for me, and maybe the four negatives you got, or could be a positive for me. But these are based on, you know, 25 years' experience working with clients and putting this together to say what's typically going to be the impact. So, when the pebble hits the pond, we know that it's going to make a ripple. What's that ripple going to do when it hits the bank? Right? So, let's jump into that.

The first one, clear definition. I think it's a very positive thing. We've been begging this for a while, and I cannot tell you how many times I've been across the table with HHS, OCR, or even a privately-hired assessment or investigator, and we're arguing over the finer points in this. Hopefully, the intent is, that we now have something that's clear, very dogmatic, in a sense as, it should be this, or it shouldn't be this. So, when you provide a document, or there's a definition of a document, we can both – the federal government and your partner, like PYA – can look at that and say, it's clear what this is and here's what I believe based on the other guidance. And once you put in the new proposed rule meets that, or to our clients, it is clear what you have here doesn't meet that, we need to help you get there, get what you need to get there, because the rule is now very clear on the definition of this. So, I think that's a very positive.

Audit and reporting? Absolutely, it's going to make that process a little faster. Now, depending on your profession, you may say, well, that's not necessarily a positive, Barry. Because sometimes having a little extra time to gather the things up, or if the mother-in-law is coming over, maybe a couple extra hours to clean the house, is always warranted. I get that. But as an industry, I think it is overall a positive thing to clean up exactly what's required and what's no longer addressable but needs to be in that audit reporting period.

Enhanced preparedness. Absolutely. The clearer definitions, along with the audit reporting specifics, are going to make it so that you're more ready. They're pushing you. I would look at it is as a coach that is making you run that extra lap, knowing that your legs are going to hurt, knowing that you're going to run out of air, and that when you actually do get in the race, you can sustain through that race. Because you're going to be, if you meet this, and we're going to talk about some things to do that you can do to prepare for this, do it. If you get there, you're going to be much better prepared for if you have some type of either a proactive audit or a reactive audit based on someone's complaint or a breach response.

And then the standards. Let's face it, we've not had a lot of security standard updates in a long time. So, this is a no brainer. It's absolutely – you know, I was looking through a document, and it wasn't that long ago, and it was a guidance document from an agency and it had in there, “make sure you're looking at the removable disc”. The floppy. It literally said “floppy disk”, and I'm like, oh my gosh. So, we're going to get a little more relevant, right? We're going to talk about it, that's why Internet of Things is in there. This is really prepared or helping us prepare for those things that are more current in the world that we live in today, and not trying to reinterpret things that were really meant for when none of this was even an idea.

Increased costs. So, these are some of the impacts. I call them challenges, right? Not necessarily negative, but potential challenges. Look, if you are a very rich system, and I know that's relative, right? And I'm not necessarily saying that being a big, rich system is a bad thing, because that allows you to provide care for more people and quality of care, and it all runs in it. I get it, but when you're looking at something that is an unfunded mandate, which this is. HIPAA is it's not meaningful use, it's not interoperability, it's HIPAA. HIPAA from the beginning and currently still, is an unfunded mandate that is agnostic of your size and ability to meet the standards. Again, in comment period, maybe you want to say something about that, right? If you're a rural hospital, a single provider practice, you're still going to be held with the same standards. It could cost some people. It could cost a lot of money to get to where the bar is currently targeted to be set. So, there's going to be some cost increase, without a doubt.

Vendor management. I just don't know how we're going to be able to do some of the downstream vendor, third-party. I do know that there's some light at the end that tunnel. So, maybe a little positive spin on this

challenge. There are AI tools out there, and again, if you guys would like to have another discussion around this, around the acceptance, send your feedback. We would put together a really nice detail on the exceptions that you can lean on in these cases, and this is one of those. It doesn't get real specific on how you're monitoring these vendors. There's some wiggle room around the vendor management piece, and there are already AI tools out there. That is a paid subscription, it's not a bank-breaker by any means, and you can put that technology vendor out there and it comes back and says here's a here's a risk of that the score. It could very well be that that's going to meet the expectation. We'll know when the final rule comes out, but right now, there's some room there and exceptions. But otherwise, if you're having to, if I'm responsible for validating your responsibility, that just in itself is full of all kinds of risk and challenges for managing that.

And then noncompliance. Obviously, the biggest challenge and the impact is if you just can't get compliant. And I don't mean that overall, I mean in time, right? So, there's a six-month grace period, and we expect from those that I've talked to and stay in the circles around the privacy and security sector and inside the Beltway, so to speak, probably ‘26 timeframe in there, unless something changes. But there's a lot of people pushing back to say, look, just pull this thing back in. There's emails coming from all over the place, as well as the public comments. They look, pull this thing back in, try again. They're focusing on few areas, and we'll talk about a couple of those as we go to the preparedness piece.

And then it's just, it's just so much at once, right? Now again, if you are a heavily budgeted, in other words you've been planning for this for a while and you've already been chipping away at it. If you're one of those, good for you, that is awesome. You're going to have less time, and it's not going to be as overwhelming, because you have been prepared. If you're a small organization with a very tight budget and your primary concern, as it should be, is making sure that patient is taken care of, and that you can collect bills appropriately and keep the lights turned on, and keep the families fed that are employed by you and support your community. Maybe some of this stuff is not the top of the budget piece of it, so it could be a bit overwhelming, and not only cost-wise but, you know, you can even outsource all this stuff to get done. But you still have to interact with it. It's still going to change. Your workflows are going to change in some places, your IT departments may grow, it is going to be, it could, for some folks, just be a little bit overwhelming. Plates spinning all over the place, and again, you drop a plate, you drop it, that noncompliance, and that's only going to make the situation worse. So, there's some concern there.

So, strategy – so, this is, this is the cool part. I'm doing a time check, and we’ve got about 15 minutes, I can get through this in 15 minutes. Okay, some strategies for you. So, let's talk about some real-world things. And again, the link that Erin shared with you of our two resources, the one that kind of paraphrases or mimics the New Year's resolution, read that, it's a fun read and it has some really cool things in there in terms of how you might prepare. Your risk assessment, start looking at those already, and there's probably some things in the industry from a standard. Look at, take the risk analysis that you're currently getting done by whomever, internal, external, whatever, and compare it to NIST SP 800-30. Of the things that we find missing, is that you really have to identify all the devices and all the applications and how the risk ranking is. Again, the threat, the likelihood of the threat giving you the result of the risk ranking. Do you have that somewhere attached into it, or at least in your work papers, is that something you can produce? Remember, federal audits in most cases, unless it's a real big complaint letter with an attached affidavit or something through HIPAA, most of the audits start with a desk audit. If you've never been through a desk audit, you don't get to say a whole lot. It's a portal you go to, and it says, upload the last six years of your security risk analyses. It doesn't say, make sure you include all of the scanning tools and

log files and all this, it's just upload it. And then there's a series of those, and you get to upload it, and then you hit submit, and there's not a lot of room to say, but let me explain, officer; let me explain, attorney. No, no, just upload it and we'll get back to you. So, make sure you're looking at your risk analysis, identify the vulnerabilities. Make sure it's done properly, because likely you're going to be compared to a much higher standard when this rule is finalized, because that's what the investigator is going to use for the criteria. For all of those of us who are auditors, we know good, clear criteria makes for a good audit, unless you can't meet the criteria. All right?

Enhanced training – I won't cover what Erin's covered I will simply say the following, you cannot train enough. To the point that if you do it the same way, every time, it's going to get noise, and boring, and not be effective. So, here's my challenge for you in this enhanced training piece, look for creative ways to train. Do some research around Game Theory. Look for ways to engage the audience, reward the audience, make it part of the full education within your health systems. Make cyber security, make compliance with HIPAA as important as hand washing or sanitizing surgery equipment, so that it's that education is at that level. Because up until this point, for most of us, it's simply been a burden that we have to go through. And we look for online vendors who put out these vanilla things, or we create something inside, "watch this every time…." You got, we got, to get better at it as an industry. We simply got to get better at it.

On the vendor oversight. You need to start an inventory of that. Look at some options, some of the AI tools that are out there, I like those. And start what that process looks like. And again, if this is something you're like Barry, we're just trying to make sure our pneumonia cases are taken care of. We're trying to make sure MRSA doesn't happen in the hospital and patients go home safely. Great. There are firms like PYA and others that can help with that piece. Get some advice there and get it soon, because the runway to get that done could be quite lengthy. Don't wait to the last minute. And these are not things where you can have, you know, giant six-figure engagements coming. No, no. These are small advisory engagements. We do tons of those, and it's some of our favorites, so please reach out there for the education and the advice.

The resources. You may need to enhance those internally, as Erin so eloquently pointed out, it is a continuous process, right? It is not something that is a point in time. It is more like the standards that we see in finance and banking around SOC-2 audits and things like that, to where we're looking for is, how has this worked out over entire year? And that hits your monitoring, your policies, your audit, your procedures. It is a continuous, we like to call it a program, right? In fact, internally, we have something called an Overwatch Program designed just for that. It never really goes away, right? It's that foundation that stays there, and it has peaks and valleys, okay, based on what's going on around it at the time. And in some of those peaks and valleys, there could be cost associated, but there's resources as well. You need to be able to flex up to those resources, but you need a steady set of resources to get you from one end to the other. It is no longer, hey, it's that time of year. That vernacular has to go away. All right? This is something that the federal government expects us, and again, I think, is a positive that we should be worried about all the time. It's no different than some of the things that we do in our clinical setting. That's just a foundation of protecting our patients. This is a foundation of protecting the data that are associated to those patients.

Incidence response plan. Erin touched on that real quick. My thing is, you don't have to boil the ocean on an incidence response plan. Start very simple, get a core group together. In that core group, legal, compliance, clinical, business operations, IT, and then some maybe ad hocs. And just start talking, if this

happened, what would we do? And see how big that snowball starts to get and then start to organize that conversation into some documents. And in those documents, it is very important to have very specific roles, I like to say, an instance response plan should look like a notebook. Back in 1997 I had one with the Six-Million Dollar Man on the front of it. It was my favorite notebook, and I had color tabs for every class that I had in junior high school. Okay? I My math was green, my language arts was yellow, my history was…all this. Your incidence response plan, in my opinion, should look similar to that. There's a tab for public relations and marketing, there's a tab for legal, there's a tab for administration, there's a tab for IT, there's a tab for nursing, there's a tab for inventory. Everybody's got a role, and if the incidents happen, you just turn to your chapter. And in most cases, the beginning of that chapter is going to be very similar for everybody. Sit still until Legal tells us what to do. Don't use the word “breach”. We will convene and let you know. And then, once the triggers pulled, there's likely some action in there. Break it down into something that can actually be done. And once you get your arms around, you say, I think this is pretty good. If you want validation, reach out to us or somebody like us. We'll tell you that that makes sense. That doesn’t make sense. You don't have to boil the ocean. Let me add a couple of things. The next phase, testing. We have what is called in the industry, a tabletop exercise. And there's agencies, the cybersecurity, infrastructure security agency, they can come in and do that, some stuff for you, free. We have products that we do that where we can facilitate those from a department level all the way up to an enterprise academic medical center. From one end to the other, right? One takes a lot longer to prepare for and get done, but they all have similar things in common. That is, how do we respond appropriately, and how do we recover, and what did we learn to prevent the next one, right? Flex that muscle. The analogy that I use is if I put you in a chair and taped your legs to that chair and I left you there for eight hours. I took care of you, I fed you, everything's great. You're just having to sit. You're relaxed. I give you Netflix, and you're going crazy with Breaking Bad, and all this stuff, everything's great. And then all of a sudden, I untape your legs and I say, the room is on fire, run! You're going to fall flat on your face because you have not exercised any of those muscles in eight hours. Think of your incidence response plan like that. If you don't exercise it, when the incident happens, you're going to fall flat on your face because the muscle is just absolutely weak. Practice, practice, practice.

And then lastly on this, I'm talking to my leaders here. If you're an executive in these organizations, it you it is not something that you provide oversight to. It's not something that you peer into. It is something that you are involved with, because you have a role to play. There's a lot of moving pieces that are going to have to happen, and you slow it down. We, I'm an executive, we slow it down if we put too many hurdles in front of that. And you need to understand, as an executive, get your leadership engaged. Okay? That needs to be part of the whole process. All right, informed communication across but everybody knows. I don't care what the process is, what the project is, Tone at the Top matters a whole lot. So, leaders, fellow leaders, colleagues, let's get involved and help get this done. It is not an IT problem. It is not a legal problem. It's not a compliance problem, okay? It's not an opportunity for one group to succeed. It is an all-in or all-fail situation. So, that's your incident response. You get everybody involved.

Now look, I once again, recommend that you do some additional education. Look at your exceptions, and if there's something that doesn't bother you, right? If there's something that bothers you and you think this is really going to be impactful for us, send a comment in for that. I'll give you an example. There's one out there that I have commented on, and I'll share it with you. Okay, the thought that you only have to do network and monitoring every six months, and then do a vulnerability test annually. All of my IT friends are going, that's nuts. And then there's an exception that says, well, if you can't do that, then maybe you don't have to do it at all, or you do it a lot less, maybe once a year to six months. Network monitoring, let

me go on the record, network monitoring is continuous. Okay? People are knocking on your door all day long, and if you're not sitting, not sitting there looking through the peephole, somebody's going to get in. Network monitoring activity, it's continuous. I don't know why it's in there, personally, every six months, but that's something that I feel strongly. At least letting the federal government know, what are you thinking here? Right? Maybe there's a reason for this, and it could be trying to get a utilitarian approach to something this large, because HIPAA is massive. Okay, maybe that's where they're at. What I would say is maybe just give those a little more time and a little money to get up to the standard. Don't adjust the standard. My recommendation to you is, get to the standard, don't rely on the exceptions. Do whatever you got to do to get the standards that's going to be important going forward. I've got five minutes left. Erin, is there anything else that you would like to add before we start to close it up and I turn it back over to our facilitators?

Erin Walker 55:35
No, sir. Thank you.

Barry Mathis **55:39**

Okay, I appreciate your attention. There's a lot of you out there. Again, this is not meant to be a certifying class. There's a lot of things that we could have talked about here. We kind of bubbled up what we've experienced over the years and what we think is worth you started with, continue the education. This is the beginning, not the period at the end, and we are more than happy to repeat some of these and go deeper. If you'd like for us to do more, give us your feedback, we're happy to do that.

And then if you'd like to see the exceptions, I think some of them are worth talking about. We could put together a presentation like this, just on the exceptions, and you can come prepared for that. And we can do a lot of Q and A, make it however you want. We're here to help. Bottom line, we're here to help. And when we try to go through this, getting prepared for it, there's a lot of people going to need that help. I'm excited about being able to do that. So, thank you very much for your time. We appreciate it. I'm going to turn this back over to our facilitators, who have done a great job putting this on today.

PYA Marketing **56:38**

Thanks to our presenters, Barry and Erin. Later today, you'll receive an email with their contact information and recording of the webinar. Also, the slides and recordings for every episode of PYA's Healthcare Regulatory Roundup series are available on the Insights page of PYA's website, pyapc.com. While at our website, you may register for other PYA webinars and learn more about the full range of services offered by PYA. Please remember to stay on the line once the webinar disconnects, to complete a short survey and post any questions you may have. On behalf of PYA, thank you for joining us. Have a great rest of your day.