WEBINAR TRANSCRIPTION

Consent Models in the Context of PHI, Behavioral Health, 42 CFR Part 2 Regulated Data – the HIPAA Privacy Rule

October 25, 2018

Hosted by

SHIEC Strategic Health Information Exchange Collaborative

Presented by
Jenn Behrens
Partner, EVP Privacy, Kuma

KUMA

Jenn Behrens:

Thank you, I really appreciate the opportunity to present to you all and share some of the information that I am somewhat familiar with and learning. This area is constantly evolving, and so that's one of the things that I enjoy, working with HIE's and healthcare organizations. It's learning how to navigate some of these nuances of the HIPAA Security and Privacy rules and the differences between consent models, and all the different types of data, and the regulations that are around them.

What we're going to focus on today is, are some different types of consent models that HIE's may use and do use in the context of various types of data, including PHI, behavioral health and data regulated by 42 CFR Part 2.

I would like to make a shout out the HIPAA Privacy world, the HIPAA Security world tends to get a lot of the attention between the two, and this is where the HIPAA Privacy

role really shines, and can be looked at a vehicle for you all to manage your consent process, and to stay informed about it. So, when you think about consent and healthcare, what you're really thinking under the regulation is about the HIPAA Privacy Rule.

With that said, I echo Sharon in that please put questions in chat. I know last time we forgot to look at the chat, I promise we'll peek at the chat towards the end. But also, I do want to hear from you all at the end and see what you all are doing, and exchange some thoughts about what practices that you're seeing, the good, the bad and the ugly.

With that, just a brief overview about who I am. I am Partner and Executive Vice President in Kuma. We do privacy and security consulting. I spend a lot of time working with organizations in the healthcare domain from HIE's to clinical research organizations, medical research organizations. I actually come from a social work background. I spent almost upwards of 15 years as a social worker providing direct services, and then overseeing the information management system, in which all that raw data went and sat for our vulnerable population.

When I jumped over to cybersecurity and privacy, it really resonated in my brain that protecting the information of those people's data that we have in systems is just like the job I was doing with the clients that I was serving as a social worker, wanting to have them at least the same as, if not better, when they left my services as when they started.

And so I very much carry that through in my work as a consultant or CPO for organizations, or if working with you all with HIPAA risk analyses, or any other type of work. And certainly in supporting your efforts and understanding some of the nuances, like I said, of this HIPAA Privacy and Security rules.

I do want to again remind everyone that I am not a lawyer, and consent can definitely fall in the realm of needing legal expertise and consultation and representation. I want to make very clear, make sure that everyone knows very clearly, I am not an attorney. I have not gone to law school at all. But I do enjoy and love HIPAA as a law. I think it's a beautiful law. There's a lot of great implementation specifications. And I like to help organizations understand how to use that as a vehicle as opposed to a barrier.

With that said, this is the agenda that we have for today. We'll go through some of it. Some of this is a little bit of a recap from our last session, which was part one of this, and then we're going to dive a little bit more into consent and authorization, what does the HIPAA Privacy Rule provide, as far as guidance. What are the difference between opt-in and opt-out, because that could be a little tricky for an HIE. And what are some consent models that HIE's are looking at using.

To frame our conversation, I wanted to really level set on why we're here. We all know that sharing individual health information is an important part of delivering quality healthcare. Healthcare providers need to be able to share different kinds of health information with other healthcare providers for those PTO, payment, treat and

operations for healthcare. Some of our federal regs, and increasingly some of our state regulations, are requiring specific consent mechanisms, which also can be sometimes more accurately referred to as authorizations for the distribution, the disclosure, or access of particular elements of an individual's health record, or the types of data that are involved in those health records. And those can involve behavioral health services, substance use disorder, and any other data that might be regulated by 42 CFR Part 2.

And increasingly in state's some additional types of information, such as HIV, or our genetic information, is further regulated beyond HIPAA. And so this is the second of a two-part webinar series. We had the first one, I believe it was October 9th, and I believe that the recording is available via the SHIEC and Kuma websites. That one really reviewed more of the specifics of the types of data, and the interplay of the different regulations, and what requirements were placed on HIE's if they wanted to exchange those types of data.

Today we're going to really dive further into consent, authorization, and the role of the HIE in managing consent, and the exchange of that patient data.

The goals for today in the session are to review the different types of data, talk about the difference between consent and authorization, because sometimes those can get murky. What's opt-in, what's opt-out. And when you say you're an opt-in HIE, does that really mean you're using an op- in model or not? And different versions of HIE consent models. And how consent and QSOA's are involved, or how they need to interact with on another.

Again, as a baseline, this is an important topic, especially for the exchange of those non-traditional PHI elements. Your mental health, and your data regulated by 42 CFR Part 2. Adults frequently have co-occurring physical health and behavioral health conditions. We know that there's a staggering frequency of patients that have comorbidity disorders. I know this from my time as a social worker. Nearly every client I worked with, had some degree of multiple disorders that they were diagnosed with that fed off or impacted one another.

We also know that patients with comorbid diagnoses are more likely to have an increase in physical health issues. And these treatments and care, so their visits to different hospitals or healthcare organizations for these disorders, may not be readily available within one EHR, or one PHR, and the exchange of the records throughout the network can provide a more comprehensive view of the patient for the treating provider.

As a recap from our last session, I did want to make sure that we review some of these definitions because I know that this space is very lingo heavy, and I want to make sure that we all have an understanding of as we're moving through this session, what the different terms refer to.

Protected health information is probably the most common one that everyone's familiar. Generally, this refers to demographic information, medical histories, tests, lab results,

insurance data. It's the information that a healthcare professional collects to identify an individual to provide that appropriate care.

Where it starts to get a little bit tricky, I think, at least in my head, behavioral health is the term that is more preferred to the label mental health, as far as the data type. However, behavioral health, and I'm using air quotes that you can't see, but behavioral health refers to the collective of the emotions, behaviors, and biology relating to a person's being and their ability to function in their everday life and their concept of self. And so culturally we have a preferred term to use behavioral health. Although this largely refers to mental and emotional health. Also, and above and beyond what protected health information generally applies to.

The next most common term that gets thrown around is 42 CFR Part 2. And so people typically refer to this, or it is used as a type of data. That phrase is actually the code and regulation that refers to the type of data that is regulated. 42 CFR Part 2 is actually a regulation that applies to records that are relating to the identity, diagnosis, prognosis or treatment of a patient in a substance abuse program.

The second part and clause of this statement is also important. This program is conducted, regulated, or directly or indirectly assisted by any department or agency in the United States. In order to be regulated by 42 CFR Part 2, you have to satisfy both of those clauses. Interestingly enough, nearly all of the programs that an HIE would encounter automatically satisfy that second clause. So you very rarely have to be wary of that regulations second clause.

Now this terms also gets interchanged a lot with Part 2, with SUD, which stand for substance use disorder, and then substance ... or, substance use data, and then substance abuse data. Notably this regulation was updated a few years ago to make a change from the application from substance use programs to substance abuse programs, so that is just something to pay attention to as well.

If you see a Part 2, or a SUD interchanged, it all refers to that same type of information.

Where does the interplay of consent and privacy and security come into play? It all comes into play in the governance that you need to make sure that you have as an HIE, in regulating who has the right to use and disclose your information. Again, this is where consent and privacy play a big role in your HIE, and that you need to understand again, this is where the difference between the privacy and security role comes into play. Security you can generally think of as that CIA triad, confidentiality, integrity, and availability. The security rule is based off of those concepts. And largely when you do your annual HIPAA risk analysis, you are actually doing an assessment of your compliance with the HIPAA Security rule. Don't forget to every so often do a review of your consent mechanisms and your governance surrounding uses and disclosures, because that's going to make sure you're jiving with the HIPAA Privacy Rule.

Additionally, don't forget that the HIPAA Privacy Rule implicates data that is in any mode or medium, not just electronic. Your HIPAA Security rule covers all electronic PHI, HIPAA Privacy Rule includes all PHI in any form.

Okay. Where do the HIE's fit in the middle of this consent context? HIE's must have the permission to facilitate the exchange of regulated patient data amongst organizations. The rub, and this is the tricky part here is that, HIE organizations do not actually mange the consent process. So the implication is that HIE organizations should have a model that your base community, so your stakeholders and within your network, your participants that are onboarding into your system, that they will easily adopt. Or that they have adopted already, and are willing to utilize with you.

Now as HIE's are more and more looking at cross jurisdictional and regional, and exchanges across the national forefront, you need to also consider what your consent models are going to be between those greater HIE associations and groups. And so, making sure that you think through those is going to be invaluable, so that you don't hit barriers downstream.

Where I say the rub, in the fact that HIE's do not manage the consent process can be a very tricky area. Some HIE's have participants who are very transparent and open, and work hand-in-hand. Some have just more aspects into their relationship. And so the more that you can work with those stakeholders in order to have everyone agree on the same model, the better you can be. What I want to make sure, again her I assert is that I'm not an attorney, but this is likely where you would want an attorney to help, if you are looking at or considering offering up some recommendations to the consent process.

If the HIE's do not manage the consent, who manages the consent? Those are your providers. Those are going to be your covered entities that are providing the care to the patients. They can appreciate that that provider is going to want to maintain legal responsibility and accountability for that consent. However, as the HIE, you need to know that you have the right consent process from the patient to that provider to exchange the data. Not only from that provider to the HIE, but from, you and the HIE's that hub, out to other organizations, other participants.

And so, this process can get very complex in how to navigate that with you stakeholders. And so understanding more of the differences in consent and authorization and that the challenges of various opt-in, opt-out models, is going to be key when you walk into those conversations.

I have discovered in my working with organizations that one of the most common misnomers is the difference between consent and authorization. The two terms get thrown around a lot and often simultaneously. This is a little bit of one of my pet peeves in that HIPAA very clearly delineates the difference between consent and authorization. In a nut shell, a covered entity voluntarily obtains patient consent for uses and disclosure of protected health information for those PTO, treatment, payment, and

healthcare operations. Covered entities that do so have complete discretion. This is all on the provider to design a process that's best suits their needs.

This is where different stakeholders are going to develop different flavors of their own consent process. And this is where as you start working with your stakeholders and your participants, you might be able to influence some of that process to make sure that it satisfies the requirements of you as an HIE in order to distribute and have people use and disclose that information further.

The difference here between consent and authorization, is authorization is the step it takes that provides that permission for use and disclosure of information that goes beyond treatment, payment and healthcare operations. So there are a lot of different types of activities that can be covered by authorizations. Some include authorizations to different people who a patient might want to know. For example, if a school system or, a social services agency, or you might look for an authorization to provide information for marketing purposes. That's definitely outside the realm of treatment, patient and healthcare operations, but also in certain context and situations has a very valid use. However, in order to use a patient information that's not anonymized or aggregated somehow, you do need to have that very specific authorization.

How you do need to have that very specific authorization. And this authorization is a very different document from a consent. It is a detailed document that gives entities explicit permission in writing to use the protected health information for a very specific purposes. So explicit and specific are two terms that you want to think about when you're talking about authorization. Explicit means that it is written out, it's not vague, and your specific purpose means there is a very tightly controlled situation in which this information may be shared.

So how does an authorization form differ from just a consent form? Essentially an authorization form has many more aspects to it that need to be very explicitly disclosed and authorized by the patient in language that they can understand. And so some of the elements that must be included are the description of the protected health information to be used and disclosed, it cannot be a blanket, "My entire patient record can be shared." That's not what an authorization is. Again, very specific. It's about the person who's authorized to make the use or disclosure. The person to whom the covered entity may make the disclosure, and it always has an expiration date, and additionally some further information about the purpose for which the information may be used or disclosed.

Excuse me. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing the authorization. So even if a covered entity feels there is a reason for further use and disclosure that would require authorization, they are not permitted to withhold treatment from that individual if the individual declines that authorization. Again, that's different than the consent as well.

So what does the HIPAA Privacy Rule say? The HIPAA Privacy Rule permits HIEs to exchange electronic health information through a network environment depending on

the purpose of the exchange. It allows covered entities to obtain that consent in order to use or disclose protected health information for those CPOs.

Similarly--this is one of the beauties of the privacy rule--the privacy rule also provides individuals the right to request that that covered entity does not use the disclosed PHI for those reasons to an HIE. So the privacy rule offers a vehicle both for the exchange and the restriction of PHI through an HIE organization. And if that covered entity decides to pursue the exchange of information, they are required to have policies in place through which they either accept or deny requests. So the covered entity needs to track that process very closely, which should also help out with your decision as an HIE how to enable the consent process in your model.

Covered entities could design processes that apply at a more global level. For example, by requiring an individual's consent prior to making any disclosure of PHI to or through an HIE, or granting restrictions only in which none of the individual's health information is to be exchanged through HIE. Or at a more granular level, such as by the type of information, the potential recipient or the purpose for which a disclosure may be made.

So the HIPAA Privacy Rule actually can provide a lot of variants, and again, flexibility, for covered entities to decide how to implement the consent process or sharing information with the HIE. That's another reason to work very closely with your provider community to try to get to a point in which you all agree. If that organization is going to go to the more granular route, you could run into more issues.

However, you can also work with that organization so that they're doing the filtering, and that burden is not placed on you as the HIE. And there are different ways to do that through different controls that can be applied in the various staff that you have. And I've done that and I'm doing that with a couple other organizations, so I've seen it done. And sometimes that's also a way you can control your behavioral health data and your 42 CFR data as well. And you want to save more of a granular control, even if you have an overarching consent. So that can happen as well.

Okay. So what are opt in and opt out models? So this is where you need to be very careful when you're calling your approach to consent opt in or opt out. Many will say that they are an opt in HIE, believing that represents that everyone is sharing data, and less explicitly, choosing to restrict it. However, what this is really saying is that the HIE explicitly requires information to exchange the data.

So when you're considering saying whether you're an opt in or an opt out HIE, you need to understand the perspective that that statement is taking. Traditionally, the terms opt in and opt out are reflective of the individual's perspective, and not the organizational perspective. This can get a little confusing, and so while this may not seem necessarily a big deal with many stakeholders who get the connotation of what you're saying, you may need to be much more specific and clear in contracts and legal discussions, and when framing your official business model so that you can make sure you're adequately and appropriately representing the model in which your HIE is operating.

Again, the opt in opt out perspective between a patient and an HIE organization tend to be near opposites. So the actual definition denotation of opt in is that the HIE has no data until patients very explicitly give specific permission to contribute their data. The pros are to this are that it gives patients the right to protect their data from security flaws and in organization it allows patients the right to decide what storage formats are or are not secure. And patients, advocates report, are more likely to learn about the benefits of sharing their health information data if they're forced to explicitly consent to their data being shared.

Opt out alternatively means that the patient data is automatically added to the repository or into the network of exchange, and patients must explicitly request for their data not to be stored in it and for the data to be removed. This is often where the majority of public opinion lands. I saw a study out of Vermont and I don't know if we have anyone from Vermont on or who works with organizations in that state, 96% of public opinion favored the opt out model in which their patient data would be automatically added to an HIE exchange network.

The benefit of this model for HIEs is that it results in a considerable amount of ease upon administrative burden as the HIE organizations do not have to manage individual consent throughout the whole network, where if you have an opt in model, you traditionally have much more administrative overhead in managing that. So again this is one of the places where it can, where I hear HIE orgs and other stakeholders talking very quickly if I'm an opt in or opt out and then we start walking through what that means for consent mechanisms and how the patient data flows. This can be very tricky and again, often times the exact mirror of how you think you would say it.

So again the difference here is the perspective. The traditional and denotation of these terms is from the patient perspective, not the org perspective. And so just when you are presenting that information, just be careful to who you're representing and how you're representing your model.

So what are different consent models in HIEs? The goal of a consent model ultimately is to let healthcare providers look at a patient's medical history. That's the reason why we're all here with HIEs. We're trying to provide that holistic, comprehensive medical record, review, and access for healthcare providers to provide that more seamless continuity of care for our patients.

From a patient perspective, consent provides varying degrees of protection of their medical information and the different consent models provide different abilities to control and different levels of control, and who can access that medical record. Remember again, the HIPAA Privacy Rule is all about use and disclosure, so consent is all about who has the right to use and disclose that data. From the provider perspective, a consent model impacts the day to day work flow and how consent is obtained and what may be seen in that patient's medical history.

There are four broad types of consent models that are out there. There's the opt out consent, where HIEs are legally and automatically collecting information without any patient consent, unless that patient explicitly withdraws that consent. There are two different types of opt ins that generally associated with HIEs. There's that provider based opt in, so you can consider it provider by provider, and sometimes it's last in last out kind of queuing for that consent.

Then there's another approach that has the community wide consent so that the patients have consent, once they provide the consent, they're consenting to every healthcare provider in the state or community. State is used somewhat generally in this chart. I put a link to this chart at the bottom of this, and this [inaudible] will be provided to you all later. So in case you want to go look at this as well.

This particular chart calls out consent to access, which is used to New York State. I will say, and my [inaudible] provides a little bit of indication, states are increasingly starting to regulate this. And whether it's through state policy, which is an administrative control or state regulation or legislation, which is the regulatory code, states are starting to get involved with this aspect. And so regardless or what HIPAA says, don't forget in whatever state you operate, you do need to check the state reg. This is when having your legal counsel and your privacy work in tandem to discover and examine your state regulations as they conflate or contrast with HIPAA and then also 42 CFR. So you just want to make sure that you're staying on top of that.

And some of these regulations that are popping up in states can evolve very quickly. So they can move around. They can be published with AROTA, so things that are going to be amended down the line, and then again, what I'm also seeing is that if they aren't more rigorous than HIPAA, then sometimes they actually, I don't want to say override, but sometimes they don't necessarily agree with how HIPAA rights are stated. So just be very careful in navigating that and make sure that you have a good team approaching how to examine that.

Here we go. So this is another good table, and I left the titles up here. And this has all 50 states and so I wanted to give a little snapshot about the differences that are happening amongst states and how involved state governments are in HIE consent mechanisms and how there are differentiations in the scope of the consent policy. So HIEs today are doing a little bit of everything. They're using opt in models, opt out models, some are not operating with any formal policies, some have no influence from the state, some have community wide agreements, some are provider based, based on the size and scope of the providers.

So this table provides a really good quick snapshot. I would encourage if you all are looking at sharing best practices or want to see what other states perhaps in your networks that you're looking across states or national exchanges, this might be a good place to start. Again, this is how the state governments are influencing the consent mechanisms and the scope. So for example, Maine, you have a statute that is an opt out statute that applies to the state designated HIE.

However, in Massachusetts, you can have an opt in statute that applies to any plan that receives funding from a specific fund. So again, this is where this can get not only complex but complicated, especially if you're exchanging data between states and you need to somehow figure out how to have a common consent model. So understanding where policies and regulations sit that might influence those HIEs is definitely necessary, in addition to understanding what your stakeholder community looks like at home. And I can provide that link, Sharon, to that after this too.

So consent and QSOAs are also implicated with one another. Consent and authorization again may provide for the exchange of PHIs though the HIE. Remember, we're also increadingly looking at exchanging behavioral health and 42 CFR part two regulated data so that we can provide a much more comprehensive and robust patient healthcare compilation to physicians and providers so that they can have better coordination of care. 42 CFR part two organizations if you'll remember require a qualified service organization agreement to be exchanged to disclose that information. So you may want to look at incorporating downstream QSOs into your consent and authorization mechanisms.

So before I go too much further, I did want to ... I do want to open this up for questions or comments. I'd love to hear what you all are doing, but I do want to just do a really quick summary of what is a QSOA. Because that's another somewhat complicated term and can be interpreted a couple different ways. So a QSOA is a qualified service organization agreement. So this is a specific contractual mechanims that permits the disclosure of information between a part two program-- so remember, a part two program is a substance abuse program that is funded by the federal government-- and an organization that provides services to the program, like an HIE.

So this covers organizations that are storing patient data, that are receiving and reviewing requests for disclosures to third parties, and facilitating electronic exchange of that patient information. Notably, 42 CFR part two data may only be made available for exchange for treatment. So this is again where we're looking at the difference between consent and authorization, too. Remember, consent covers PTO, the whole patient treatment operation gamut. 42 CFR part two data may only be exchanged for treatment purposes.

And so when you're looking for your how to invoke a QSOA with patient consent, you need to understand interplay. An HIO or HIE may disclose part two information that is received from a part two program to HIE affiliated members, so those downstream HIE participants, so those are the ones that are different than the original part two programs through which the patient is a member of or is getting--

Unto which the patient is a member of, or is getting care from, only if the patient signs a part two compliant consent form. Patient consent, however, is not needed to authorize such organizations between HIE and Part Two Program, when a QSOA is in place between the two. So when you're structuring your consent or you're navigating that

conversation with you're participant organization, you want to think very carefully about if you're going to be exchanging data that's regulated by 42 CFR Part 2, and if you want other organizations to have access to that, and again, this is the use and disclosure, so you want to think through how you structure your consent programs with your provider organizations that also supplement a QSOA agreement.

So this gets back to where I started, where working with your participants to understand whether they're truly an opt-in or opt-out, then how their consent or authorization vehicles are worded. You all want to have a consensus on that approach, and then you may want to offer suggestions or thoughts on ways that consent can also include ... that the provider consent forms may also reference and include behavioral health and 42 CFR Part 2 regulated data that could be used in conjunction with Qualified Service Organization Agreements, and then when you're doing that consent form, consider the way it goes, whether it's opt-in or opt-out, and if you want to have the patient have the ability to do the opposite, then how would that form look like, or what would that form look like, and then how would that be managed? And is that provider by provider? Is it that patient by patient? Is that community-wide? And because that's going to implicate how the use, how that information is used and disclosed throughout your network.

So this is where this can become very tricky, but if you parse it out, sometimes honestly with the opt-in, opt-out things, getting on a white board or putting this on a piece of paper can also help when you're trying to flip between the patient perspective of opt-in and the HIE perspective of what they can connotate opt-in is referencing.

So, be very careful when you're looking at the flow of data based on consent models, and who is maintaining that consent. Again, an HIE traditionally does not manage the consent process, but something you want to navigate with your providers, but you want to understand that everyone has agreement into the model that your community minimally is using, and then you want to understand how that implicates your greater network, if you're part of a regional HIE or part of the, or if you're rolling up to a national HIE.

And so, all of that consent and authorization, those mechanisms also, if you're looking at sharing this highly-regulated data that's regulated by 42 CFR Part 2, please consider a QSOA and putting that in place not only with the provider that you're receiving the data from, but those providers that may be using that data as well, so that you have covered your liability further and have more clear understanding of ... you may ask us what ... then don't forget to check your state regulations on top of that.

You may need additional statements in your consent that you can navigate with your providers, or in your QSOA, and so again, this can be very complex, but if you start to deconstruct it and walk through the use case and the data flows and where patient consent resides, then you can start to come up with your baseline consent model that you can feel more comfortable in articulating and getting buy-in from your community members.

So, with that said, we have about 15 minutes. I would love to take questions or hear comments, and also definitely, I would really like to understand what you all are doing right now in your HIEs regarding consents, and so, Sharon, I'd love to open up the lines. I think one of the best ways to learn about this and HIEs is to share what other people are doing.

Thank you, Jen, and thank you for the presentation. At this time, if you have questions for Jen, you can either put them in the chat box, or please go ahead and unmute yourself and ask your question. Please let us know where you're at, and your name, and which organization you're with. Go ahead if anyone has questions.

Anyone have a question? Or does anyone have ... are you willing to speak up and talk about where you're at in the process with your particular HIE? Do you have this information in place at this time?

Hi, this is Janet Harriot, Quality Health Network in Colorado, Western Colorado, that is, and I'd be certainly happy to share our experiences. It may be more of a lengthy discussion than you have time for now, but I think, suffice it to say, we've been receiving part-two data for two years now from two different substance abuse treatment facilities, and it was a long project that took a lot of cooperation from many parties, but the motivation really had to come from, pretty much from the community.

The medical providers were asking for more information, better communication from our substance abuse treatment centers, and they're the ones that really pushed for this, and that's how we got them, the substance abuse treatment centers, on board and at the table, working through everything.

It was certainly not top, or driven by the HIE. We were certainly there at the table and helped get it all figured out because they need us, but that's probably the most important point is that it's got to be driven by the community.

Agreed. Very good point.

This is Sharon. I have a question to that end. How were the providers receptive to the HIE concept? Was that part of the issue that may have been complicating things, or were they accustomed to working with the HIE?

Oh, no, yeah. QHN's been around for ... since 2004, 2005. No, QHN's been in place for a long time. That wasn't the issue. The issue is: they could never get information from the treatment centers in a timely fashion. When they asked for it, they couldn't get it, especially in the ER. No. There was no information coming in to QHN at that time from these treatment centers.

So we were the vehicle that made sense.

Okay, thank you.

Does that answer your question?

Yes. Thank you.

There was a question in chat, Sharon, about whether we'd share the spreadsheet of what other HIEs are doing. I think this is referencing the chart that I had in there, and, yeah, I'll dig up the link to that chart, and I'll provide ... I'll go ahead and put that on the deck, and then also provide that to you, Sharon, so that can be shared.

Alright, thank you, Jen.

You're welcome.

Other questions, or anything you would like to share with the group?

Hi, this is Christy Schmidt. I'm from Michiana Health Information Network in South Bend, Indiana, and I'm just struggling with understanding, differentiating between 42 CFR data and just general behavioral health data, and how does that ... where does the consent lie if it's just general behavioral health data, versus the 42 CFR?

Yeah, that's a good question. That was ... and, Sharon, I think the first webinar's available, and that was the, more of the focus of the first webinar, but in brief, behavioral health data is largely regulated by HIPAA, and so with a few exceptions, behavioral health data can be exchanged in accordance with HIPAA guidelines. Some of this has to do with your risk tolerance for exchanging this type of information. Also, this is where state regulations are getting increasingly complex in regards to protected health information.

So state regulations are actually starting to regulate the behavioral health data above and beyond protected health information, so this is an area you would definitely want to check with your state guidelines and state legislation to double-check to see if there are any further implications with behavioral health data. At the state level, above and beyond, 42 CFR Part 2 is generally considered the most highly regulated type of information in this sector. So that's where you get into the explicit consent and the QSOA in order to exchange that type of data, where you don't necessarily need to have that in your mechanism for behavioral health.

Sarah, just, I know with some of the HIEs I work with, they are looking at invoking different security controls on that and then also using a more granular control in order to permit the exchange of that data within their home community versus at a nationwide level, just because of the preference of the community stakeholders and the boards that are involved, and that gets down to risk tolerance as well.

So, that also just ... once you check all the security and compliance boxes, then, to a certain degree, especially with behavioral health, it becomes more a function of risk

tolerance from a business perspective, but I would be happy to talk more with you about that and also I'd encourage you, if you have the availability to go back and listen to the first webinar, because we talked about that as well there, too.

But also happy to continue talking that one.

Great. No, thank you. Appreciate that.

You're welcome.

I have one more question on that: so I was at a SHIEC webinar a couple years ago where there was discussion about the 42 CFR data, and if that data is just elements of data that is kind of just recorded into the patient's chart from another provider, not from the substance abuse facility, and I think my understanding there is that it's then just generally treated as behavioral health data in general and not substance abuse. Is that a fair analysis?

I think probably a couple years ago, I want to say it was updated in 2015, 2016, but don't quote me on that, and I think that's where some of the delineation came into play, where, for example, they - they, and again, I'm using the air quotes - the legislature who was involved in evolving the language in that regulation, update it to reflect substance abuse program data from a US-funded substance abuse part-two program, so it's now very specific. It may have been more open before.

Thank you.

Mm-hmm (affirmative). And again, this is where I would also encourage you to talk with legal counsel, just to make sure that your interpretation is correct in your home state and with your own HIE.

I noticed on the table that some of the states have no policy on opt-in or opt-out. That's unusual. I'm just curious: how is that handled then?

Right.

So, what that chart was [inaudible] was also the state's involvement, so if you'll remember, and from the first webinar, I had a graphic where it said, you know, it was looking at the continuum of restriction on how you would handle data. 42 CFR Part 2 is the most restrictive, while HIPAA is the least restrictive, honestly, which I think is shocking to some people. In the middle, there tend to be state regulations.

So, increasingly, states are hopping in on the how you can share data and why, and so some states are forming official administrative policies, and some are ruling on legislation that inform and require how consent is invoked by an HIE. Some states have chosen not to wade into that territory or haven't come to consensus into a policy or legislation, so I suspect that as time goes by, and HIEs become more adopted, we'll see

more of those, but you're right. And that was part of why I showed that particular section, because there's such variance, and so really understanding your home state and then the states in which you inter-operate with is going to be very important into understanding what type of consent model you can move forward with or the types of controls you need to invoke in your technology stacks.

Sharon:
Thank you, Jen, and thank you for the presentation. At this time, if you have questions for Jen, you can either put them in the chat box, or please go ahead and unmute yourself and ask your question. Please let us know where you're at, and your name, and which organization you're with. Go ahead if anyone has questions.

Anyone have a question? Or does anyone have ... are you willing to speak up and talk about where you're at in the process with your particular HIE? Do you have this information in place at this time?

Webinar Guest, Janet:
Hi, this is Janet Harriot, Quality Health Network in Colorado, Western Colorado, that is, and I'd be certainly happy to share our experiences. It may be more of a lengthy discussion than you have time for now, but I think, suffice it to say, we've been receiving part-two data for two years now from two different substance abuse treatment facilities, and it was a long project that took a lot of cooperation from many parties, but the motivation really had to come from, pretty much from the community.

The medical providers were asking for more information, better communication from our substance abuse treatment centers, and they're the ones that really pushed for this, and that's how we got them, the substance abuse treatment centers, on board and at the table, working through everything.

It was certainly not top, or driven by the HIE. We were certainly there at the table and helped get it all figured out because they need us, but that's probably the most important point is that it's got to be driven by the community.

Jen: Agreed. Very good point.

Sharon:
I have a question to that end. How were the providers receptive to the HIE concept? Was that part of the issue that may have been complicating things, or were they accustomed to working with the HIE?

Janet:
Oh, no, yeah. QHN's been around for ... since 2004, 2005. No, QHN's been in place for a long time. That wasn't the issue. The issue is: they could never get information from the treatment centers in a timely fashion. When they asked for it, they couldn't get it, especially in the ER. No. There was no information coming in to QHN at that time from these treatment centers.

So we were the vehicle that made sense.

Okay, thank you.

Jen:
There was a question in chat, Sharon, about whether we'd share the spreadsheet of what other HIEs are doing. I think this is referencing the chart that I had in there, and, yeah, I'll dig up the link to that chart, and I'll provide ... I'll go ahead and put that on the deck, and then also provide that to you, Sharon, so that can be shared.

Sharon: Other questions, or anything you would like to share with the group?

Webinar Guest, Christy:
Hi, this is Christy Schmidt. I'm from Michiana Health Information Network in South Bend, Indiana, and I'm just struggling with understanding, differentiating between 42 CFR data and just general behavioral health data, and how does that ... where does the consent lie if it's just general behavioral health data, versus the 42 CFR?

Jen:
Yeah, that's a good question. That was ... and, Sharon, I think the first webinar's available, and that was the, more of the focus of the first webinar, but in brief, behavioral health data is largely regulated by HIPAA, and so with a few exceptions, behavioral health data can be exchanged in accordance with HIPAA guidelines. Some of this has to do with your risk tolerance for exchanging this type of information. Also, this is where state regulations are getting increasingly complex in regards to protected health information.

So state regulations are actually starting to regulate the behavioral health data above and beyond protected health information, so this is an area you would definitely want to check with your state guidelines and state legislation to double-check to see if there are any further implications with behavioral health data. At the state level, above and beyond, 42 CFR Part 2 is generally considered the most highly regulated type of information in this sector. So that's where you get into the explicit consent and the QSOA in order to exchange that type of data, where you don't necessarily need to have that in your mechanism for behavioral health.

Sarah, just, I know with some of the HIEs I work with, they are looking at invoking different security controls on that and then also using a more granular control in order to permit the exchange of that data within their home community versus at a nationwide level, just because of the preference of the community stakeholders and the boards that are involved, and that gets down to risk tolerance as well.

So, that also just ... once you check all the security and compliance boxes, then, to a certain degree, especially with behavioral health, it becomes more a function of risk tolerance from a business perspective, but I would be happy to talk more with you about

that and also I'd encourage you, if you have the availability to go back and listen to the first webinar, because we talked about that as well there, too.

But also happy to continue talking that one.

Webinar Guest, Christy:
I have one more question on that: so I was at a SHIEC webinar a couple years ago where there was discussion about the 42 CFR data, and if that data is just elements of data that is kind of just recorded into the patient's chart from another provider, not from the substance abuse facility, and I think my understanding there is that it's then just generally treated as behavioral health data in general and not substance abuse. Is that a fair analysis?

Jen:
I think probably a couple years ago, I want to say it was updated in 2015, 2016, but don't quote me on that, and I think that's where some of the delineation came into play, where, for example, they - they, and again, I'm using the air quotes - the legislature who was involved in evolving the language in that regulation, update it to reflect substance abuse program data from a US-funded substance abuse part-two program, so it's now very specific. It may have been more open before.

Christy: Thank you.

Jen: And again, this is where I would also encourage you to talk with legal counsel, just to make sure that your interpretation is correct in your home state and with your own HIE.

Christy: I noticed on the table that some of the states have no policy on opt-in or opt-out. That's unusual. I'm just curious: how is that handled then?

Jen: Right.

That chart was also the state's involvement, so if you'll remember, and from the first webinar, I had a graphic where it said, you know, it was looking at the continuum of restriction on how you would handle data. 42 CFR Part 2 is the most restrictive, while HIPAA is the least restrictive, honestly, which I think is shocking to some people. In the middle, there tend to be state regulations.

So, increasingly, states are hopping in on the how you can share data and why, and so some states are forming official administrative policies, and some are ruling on legislation that inform and require how consent is invoked by an HIE. Some states have chosen not to wade into that territory or haven't come to consensus into a policy or legislation, so I suspect that as time goes by, and HIEs become more adopted, we'll see more of those, but you're right. And that was part of why I showed that particular section, because there's such variance, and so really understanding your home state and then the states in which you inter-operate with is going to be very important into

understanding what type of consent model you can move forward with or the types of controls you need to invoke in your technology stacks.

Sharon: Alright. Anyone else have questions or comments?

Jen:
Well, I would like to ... that's me, wearing my I Love HIPAA shirt that I wore to SHIEC. I want to say thank you again to SHIEC for having me present this webinar series. I really appreciate it. I do love talking about this with organizations that have vested interest and are doing the good work that you all are doing.

So please feel free to reach out to me if you have questions or if I can chat about anything further or if I can help support your organization.

Sharon:
Jen, on behalf of SHIEC and all of the members, thank you so much for the two-part presentation and for giving us your time and expertise and everything. We truly appreciate it.

So, with that, everyone, we will say good afternoon and take care.

Listen to or **download and read** webinar one of this series, *"Privacy Compliance and Consent to Share: Understanding the Mental Health Landscape"*

About Jenn Behrens

Jenn started her career in social work as a foster care social worker. For over a decade, she moved through and up local departments of social services and landed at the state level where she oversaw some of the information management systems. Through her journey there, she started understanding research implications, data sharing implications, as well as the designs that go into building the systems that contain raw data about very vulnerable populations. She had to opportunity to jump from social service to work on a cyber security initiative out of NIST and from there, she took on the task of managing privacy – an area misunderstood throughout the industry. This led her to the world of security, privacy, and digital identity – and with that her first pilot which was about sharing information with a healthcare organization. At Kuma, she continues her work in security and privacy consulting services and with that, applies her original passion for healthcare to working with clients to integrate best practices into their organization.

The Kuma Difference

Health Information Exchanges must meet highly regulated privacy and security requirements and may not have the resources to go it alone. Kuma can help you with all your needs from the complexities of consent to HIPAA compliance to establishing a long-term program that ensures compliance today and in the future. We ensure you have access to senior level resources and confidence through our forward-thinking approach. Learn more about Kuma at www.kuma.pro.