WEBINAR TRANSCRIPTION
Privacy Compliance and Consent to Share:
Understanding the Current Mental Health Landscape

October 9, 2018

Hosted by

SHIEC Strategic Health Information Exchange Collaborative

Presented by
Jenn Behrens
Partner, EVP Privacy, Kuma

KUMA

Jenn Behrens:
Thank you, Sharon, for the introduction. I also want to give my appreciation to SHIEC and, certainly, the Behavioral Health Learning Collaborative Group for having me present on this topic. I sincerely appreciate the time.

I'm going give a little bit more about my background, so you have some context into why this is a particularly relevant subject for me, and then we'll dive into some of the subject matter. I do want to leave opportunity for an exchange of practices that are going on now, as well as to open up the floor for questions at the end. I don't know that we'll take the whole time, maybe we might have the gift of time back at the end, but I want to make sure we have that time left for discussion.

And then, as Sharon said, we're going to have a part two to this. Today will be a flow between these two sessions, and I hope that conversation and dialogue at the end of the time together today can also help craft what we discuss during the next one. I will provide the slides to Sharon to put on the secure site if anyone is interested in more of the content and referring back after the session is over.

With that said, I want to provide a little bit more background about me. Sharon did highlight some of my more recent work experience. This is really my second career. My first career was in social work. I was a foster care social worker for over a decade, and as I moved through and up working with the local departments of social services, I moved up to the state where I oversaw the Information Management System. Through my journey there, I really started understanding research implications, data sharing implications, as well as the designs that go into building the systems that contain a lot of information that is raw data about very vulnerable populations. And so, that was part of something that I took very seriously and to heart when I was there working in social services.

Several years ago, I had the opportunity to make the jump from social services to work on a cybersecurity initiative out of NIST. In this transition, I was handed the privacy work because no one else really understood it. For me, it resonated in my brain from my work with social work. It translated to, I'm still protecting the information of these systems with cybersecurity initiatives and wrapping privacy throughout the technical controls. And so, it was a natural crosswalk for me, from social work to work in cybersecurity and privacy and digital identity solutions. Interesting enough, the first pilot that I worked on was about sharing information with a healthcare organization. So very quickly into my second career, I had to tackle HIPAA, and I had to tackle information exchange of data between entities. And so, this has always resonated and been part of my privacy and security career and has been at the forefront of everything that I consider when I work with healthcare organizations. KUMA provides security and privacy consulting services, so you have that context for where I come out of now with my career.

I want to make sure that I'm very clear and you all understand, I am not a lawyer. Every so often, I flirt with going back to get my law degree, but then I calm myself back down and realize I can't go after every single degree there is. So when we're talking and working through this information, and if you ever reach out to me, I'm more than happy to hop on a call or do anything, you know, touch-ins over emails. Just remember, I'm not an attorney, so I'm not providing you with legal advice or any sort of counsel. I recommend that if you are making organizational decisions regarding consent and exchange of information, you definitely want to check with your current council, whether that's in-house or external, and also with any of your state or local regulations that may apply. We'll go into that a little bit more as to what those state regulations are, and how they may interact with how your organization needs to govern the exchange of data.

So that's a little bit about me and why this topic is in particular so important for me. We are going to try to compress a lot of information into a short period of time. We're going to do a quick overview of why we're here. What are we really talking about? Why is this important? Where do you all as HIEs and HIOs fit in? We're really going to talk about what the data says, and what the different types of data are implicated in HIE exchange for sensitive data. We're also going to talk about what the different regulations are that come into play at the federal and state levels, and then examine whether this means we can or cannot exchange behavioral health care and substance abuse disorder information. We're going to talk about some of the mechanisms that you can utilize and how those are permitted under various regulations, and what those federal regulations really mean. What's that bottom line from a federal regulation perspective? And then, look at any other nuances that you need to consider.

We'll touch on the interplay of consent with privacy and security. That's probably a more significant portion of the second webinar in a couple weeks that Sharon mentioned. And then, look at all of this and how this really comes to bear on whether your organization decides to share or not share information. And then, like I said earlier, I would really be very interested to understand how you're tackling this subject in your organizations now, if you are, if you have heard about it, what practices that you've put in place, or if you're just looking ahead and kind of examining things as they come.

So, why are we here? I don't really need to call this out too much because you all are at the forefront of understanding that exchanging health information is really important and critical to delivering quality healthcare. We know that healthcare providers share a wide variety amount of health information with other providers for those typical PPOs, so payment, treatment, and healthcare operations. Some federal laws and some state laws these days are starting to require advanced, specific consent mechanisms regarding certain types of health information, specifically behavioral health, mental health, and substance use disorders.

42 CFR Part 2 is not a new regulation. It actually dates back to the '70s, so it's been in existence longer than HIPAA, and there have been some movements of late to try to align CFR Part 2 with HIPAA. As that starts to happen, and as federal organizations and state organizations start to provide guidance, it can become a bit complicated, And so, HIEs are really at the forefront of needing to understand how to navigate those overlapping regulations, and where they may compete or interact or ducktail with one another.

This webinar is really designed to start walking through some of this information, break it apart and delineate it for you. The next webinar will start pulling apart some of the various consent models that you may utilize as you're beginning to invoke the exchange of this sensitive information.

The goals for today's session are to discuss what constitutes this sensitive, protected data, identify how HIPAA and 42 CFR Part 2 are related, and provide an overview of that security, privacy, and consent that you need to consider. I will say the overall goal is to provide some clarity around terms and definitions. This is a really very complicated matter. It's implicated by competing regulations, and even more so, by changing technology that impacts how security and privacy of patient records are maintained.

I am not by any means, providing end-all, be-all recommendations on this. Again, this is no way to be construed as legal advice. What I am seeing, and I am excited to be presenting for you today, is that this issue is becoming more and more at the forefront of conversations that I'm hearing with healthcare organizations, and certainly with HIEs. I'm also seeing confusion over different types of data, and which laws affect which aspects of the data, and which govern how you can share and through what vehicles. And so, we're going to talk a little bit about that too, because understanding some nuances are essential.

So what is the fuss about? This really is a very significant issue. Adults frequently have co-occurring physical health and behavioral health conditions. When I was a social worker, I saw this a lot. Nearly all of my patients had mental health issues and co-occurring substance abuse issues. Comorbidities we know are associated with elevated symptom burden, functional impairment, a decreased length and quality of life, as well as implicated

financial costs. The reality is that a lot of our EHRs do not currently have fields or capability to have outpatient behavioral health care visits input into them. This causes providers to miss types of data or information that could inform better treatment decisions, in addition to the quality of care being impacted by the exchange, or lack thereof, of behavioral health care and substance abuse disorder information. There's also financial implications, to the tune of tens of billions of dollars every year.

This is not a small matter. This is probably something that resonates with you all on a daily basis, and in no small degree as to why you're in the roles you are with your HIE. Where do HIEs fit? Certainly, you are the linchpin for the exchange of that critical health data. This improves the ability to provide good, quality outcomes for individuals. The terms that we hear out there a lot is that care coordination is critical between behavioral and physical healthcare in an HIE. Often, this is if EHRs are missing that information, being able to exchange data between behavioral health care organizations that provide mental health services or substance abuse disorders, can mitigate those gaps that exist in some of the current platforms that are out there.

The rationale is that access to this information helps the entire team gain a better picture of the patient's health. Providing that timely access reduces barriers to medication and treatment adherence, and also enables a better prescription of controlled substances. However, we all know that. That's nothing new. Current guidance is a bit murky. There are recommendations to exchange data in a manner that satisfies the HIPAA privacy and security roles. So, what that means is that you are recommended to exchange in a safe and privacy-enhancing manner, but that doesn't really provide you with specific permission or guidance implementation direction on how to manage that consent or exchange protocols or how to reconcile the federal and state legislation. It can get, again, a bit murky.

And so, as I'm talking with other healthcare organizations and HIEs, there continues to be the question about where does behavioral health data fit in the HIPAA sector. What does 42 CFR Part 2 really mean? And so, that's some of what we're going to spend our time on today.

What are these different terms in regards to the different types of data, and what are the nuances between them? And so, probably the one that most everyone understands very clearly is Protected Health Information. Generally, this is your demographic medical information, test results, insurance. It's something that a healthcare professional collects to identify an individual for care.

The second term that we're going to be talking about today is behavioral health data. This is where this starts to get a little bit tricky, and we start to look at different terminology. Behavioral health is the collective term for emotions, behaviors, and biology relating to a person's mental well-being, their ability to function in everyday life, or their concept of self. I know for me, when I first started hearing about behavioral health, I immediately translated this to the behaviors of a person. This term really refers to the mental health of a person or a patient. Culturally, the term behavioral health is more accepted than the term mental health, which can carry a stigma and impact treatment options or payment options for an individual. And so, the industry has adopted the term behavioral health to refer to mental health matters and treatment widely. That's one of the first tricky lingo things.

The next type of data that we're talking about is commonly referred to as 42 CFR Part 2. This is actually a regulation. It's not actually a type of data. And so, this is where this also can get a bit confusing. Sometimes behavioral health is lumped into 42 CFR Part 2 inappropriately. So again, 42 CFR Part 2 is technically the term for a piece of legislation. This piece of legislation actually applies to any record regarding identity, diagnosis, prognosis, or treatment of a patient in a substance abuse program.

The second part of this important clause is that this program is conducted, regulated, or assisted by a department or agency within the United States. That has already a complicated nuance in there that you need to look at where these programs are funded or conducted or regulated. For the most part, you can pretty much assume that you're going to be within the scope of 42 CFR Part 2 if you're dealing with a substance abuse program within the United States, but it is something you want to be aware of.

Now, some of the jargon that you want to look out for is, and I have thrown some in here throughout the presentation just to help you remember, so 42 CFR Part 2 remember is a piece of legislation that refers to substance abuse data. This can also be referenced as SUD, which is Substance Use Data or Substance Use Disorders. There was an effort, of I want to say five to six years ago, to update the term from Use to Abuse. And then, this is also sometimes commonly referred to and shortened to just Part 2 Data. So there can be some confusion among those definitions, so I wanted to make sure you understood that.

Also, to jump back to mental health data, one of the more confusing aspects of mental health data is the information that is captured in your acute care - your prescriptions, your treatment, your visit, residential treatment, outpatient programs, different types of organizations that you visit. Something that's another subset within behavioral health data are psychotherapy notes. Psychotherapy notes are any notes that are taken by that mental health professional that documents or analyzes the contents of a conversation during a private counseling session, group, joint, family counseling session. These are separated from the rest of the individual's medical records. These psychotherapy notes do not include medication prescription monitoring, counseling sessions, certain stop times, what types of treatments are offered, clinical tests, diagnosis, any sort of symptoms. That is all considered behavioral health data.

Again, psychotherapy notes is that analysis of the conversation that happens in that counseling session. That's a very special and particular sub-set of this type of information that I want to make sure that you all track throughout this as well. There are very significant constraints on that data, which is why it's important and relevant to this conversation.

So, we've talked about how 42 CFR Part 2 is one piece of legislation that comes into play for HIEs. In addition to or in contradiction, depending on how you want to look at it, there are other types of legislation in place that now regulate the confidentiality and exchange of these types of data information.

Generally speaking, there are three main areas of legislation for you to consider. HIPAA is generally seen as the least restrictive of the regulations, and then that's followed by state regulations. Typically, 42 CFR Part 2 is recognized as the most restrictive legislation, which is also interesting considering it's the oldest that is presented here.

Again, it dates back to the '70s, where HIPAA, as we know, was born in 1996 and has continued to be amended and updated with various regulations like the HITECH and the Final Omnibus Rule. Now, generally speaking, state regulations are in between the severity of restriction between HIPAA and 42 CFR Part 2. However, increasingly states are providing more narrow directives on who, how, and when organizations may exchange sensitive, protected information.

Also, when you're looking at the difference between the federal regulations, some nuances are important. You can think of HIPAA as the regulation that provides the implementation specifications on how to share data, broken down into the privacy role, and the security role. There's also the titles on codes and standards. 42 CFR Part 2, however, really focuses on whether you can share certain types of data, not how. Specifically substance abuse disorder data. This looks less at the administrative technical and physical controls of how you share that data, which is what HIPAA does, but more at the mechanisms which authorize the exchange of data. And we'll go into those mechanisms in a second.

But I want to articulate again and underscore, always check with your legal counsel, especially around the state regulations, that may come into play and exceed the severity of the restriction of any of the federal regulations.

So can we or can't we share the data? Unfortunately, the answer is, it depends, and this is where this can get a bit squishy, and you need to be very careful. So technically, behavioral health data is permitted for exchange under HIPAA. 42 CFR Part 2, again, refers back to substance abuse disorder information, and that can be disclosed to health information organizations, HIOs, and HIEs if specific requirements for disclosure of information by those treatment programs are obtained.

So there are two different ways to do this, regarding consent. You can get consent between that substance abuse treatment program, and the patient, This consent provides very explicit, written information about the consent, the permissible use, who you can share this information with, the date, if there is an expiry period. It captures up to at least and perhaps exceeding, 10 different elements that you have to have in that very explicit consent.

The other way information is permitted to be shared under 42 CFR Part 2 for substance abuse disorder information, is without consent. So in case of medical emergency, this is also more commonly known as "break the glass" and reporting of crimes to entities having administrative controls if you're doing, auditing, evaluating central registries. But what's particularly relevant for us in our discussion here, is to qualified service organizations.

So that gets to, what is a qualified service organization? And what is the agreement that may be utilized to serve as the vehicle for that exchange? So a qualified service organization agreement, or more commonly known as a QSOA, under Part 2, is that mechanism that allows for the disclosure of information between a Part 2 program, so between that substance abuse treatment program, and to the organization that provides services to the program, like an HIE.

So examples of those services may be the holding and storing of patient data, receiving and reviewing requests for disclosures to third parties, and facilitating that electronic exchange

of the information through the network. An important caveat of this is that this data may be only available for exchange for treatment.

HIPAA, if you remember, HIPPA has that PTO, so the payment, treatment, and operations. 42 CFR Part 2 is really exclusionary of payment and operations. It's really for the exchange for treatment purposes. So again, if you want to look at doing that, you need to have that patient consent that authorizes that Part 2 program, to disclose information to the HIE, and other downstream entities. Or, you have that QSOA in place between the Part 2 program, and the HIE.

And so, again, an HIE may disclose that Part 2 information if you've received that Part 2 program to HIE-affiliated numbered document or that consent document. But patient consent is not needed to authorize such communications if the HIE and Part 2 program have that QSOA in place between the two organizations. So we can look at having the QSOA in place in lieu of getting that patient consent from that treatment program if you are interested in that.

However, don't forget that you sometimes have these complicating and more severely restrictive state regulations. These are popping up now, for example, in California there's some, I think there's some popping up in New England as well. So you really do need to make sure you walk through your state regulations very carefully and understand how your QSOAs and your consent vehicles may need something modified or addressed to make sure that you can exchange this data with confidence and not with risk.

So what's the bottom line when we're talking about the federal regulations that are out there? So HIPAA does provide that you can give that behavioral health information through an HIE network as long as you have those policies and procedures in place to comply with confidentiality laws.

Remember, this means you need that PIA, so you do need that contract vehicle in place, as well as all of your HIPAA privacy rules and security rules policies and procedures. So you can't just say, yep HIPAA covers me for behavioral health information; you do need to make sure that you're covering your base.

And we're going to talk a little bit about state laws in a second. Note that if an HIE wants to exchange data regulated by 42 CFR Part 2 to an organization not obligated by a QSOA, patient consent must be in place with the originating participant organization for the exchange of that substance abuse disorder information.

So yes, you can use the QSOA between the Part 2 organization, and the HIE; what you need to make sure is if you have another participant who is looking to exchange or receive or queries that information from that Part 2 program, you have a QSOA in place with that third organization, that downstream organization.

This is where this gets really complicated. You need to think very carefully through your use-cases and sometimes taking a big whiteboard out, and drafting these things out can really help with the arrows and where do you have your QSOAs between what organizations.

Again, also remember in this, and this is one of the reasons I went back earlier, psychotherapy notes are completely different than behavioral health information, and data regulated by 42 CFR Part 2. These types of data, these psychotherapy notes may only be available in certain break the glass scenarios, and not necessarily in all of them.

Jenn Behrens: The reality is, that the current EHR platforms may restrict the possibility of actually having this information, but you should definitely, if you are talking with an organization that has this information and you're looking to exchange files or do web services, you need to be very careful and walk through the controls that are in place to segregate out psychotherapy notes from the rest of the data population.

So, we talked about the federal bottom line; the federal laws, HIPAA, and 42 CFR Part 2 apply to all 50 states. There's no getting around them. However, states are now passing their own confidentiality laws, and they're different between the states within the United States. This is really designed because different states have different tolerances for protecting sensitive health information like mental health, HIV and AIDS, reproductive health, genomic information; all those sorts of types of info are becoming specialized classes that states are really starting to pay attention to.

And certain states are starting to advance that more than others. And if you're starting to have those ... If you have organizations that are within those states that also have state regulations in regards to those types of information, you follow the most stringent, or the ones that provide the most privacy-protective laws.

On the flip side of privacy-protective, means the most restrictive to the exchange of data. So you need to really walk very carefully through all of the state's laws as to how they may supersede those federal laws. This can be somewhat tricky to how to stay on top of your current confidentiality laws within your jurisdiction and your state. Definitely working with your agency's privacy officer and your legal counsel; also tapping your State Attorney General's office.

I have found in my experience, the more you make friends with your State's Attorney General, the better, especially if you have something that goes sideways towards an incident or breach. If you've already established a relationship, and a communications cycle and pathway with your State Attorney Generals, especially if you are going to decide to exchange sensitive information in a state that has more restrictive or protective privacy laws, the better you're going to be if something does go sideways, because then you've already established a rhythm or cadence to communications, and there's a familiarity with the personnel. So I would encourage everyone to reach out and establish that relationship before things could go down a nefarious route.

There are, of course, implications to privacy and security, and how consent is then invoked based on these regulations. If you decide to share, you need to examine your methodology and your compliance of your consent model, with your privacy protections and your security controls. Consent can mostly and generally be thought of your governance and regulatory implications for exchange, while privacy covers your uses and disclosures, and security broadly looks at your confidentiality, integrity, and availability; that CIA triad of the systems that hold all the data within your system.

I do want to articulate again, do not forget your PIAs. We've talked a lot about the QSOAs in this webinar; do not forget your PIAs. This is a very important aspect of the governance, and this is where your legal really can start to work with your privacy and security officers to assure that permissible use is in place, and access is restricted.

This implicates both your program policies and procedures, as well as the technical controls in your platform. Further, just because you've determined that you can exchange and that you have 42 CFR Part 2 data on the brain, because that's what's hot right now in conversations, don't forget some of your basic HIPAA requirements regarding organizational training, access controls and differentiation between the privacy role and the security role.

So as a reminder, the privacy role really articulates the controls around uses and disclosures for all protected health information, not just electronic. So it's verbal, it's written, it's something coming off a fax machine which I wish everyone would kill if you're using a fax machine to exchange data. It's really wherever CIA might live.

So your security role really focuses on that confidentiality, integrity, and availability of your electronic CIA, so this is the data that's within your system, and it really focuses on the controls for the technology, as well as the physical and administrative roles around how you secure your systems, and the data within.

As a reminder also, and I always put this out there, please don't forget to conduct your HIPAA risk analysis, develop a HIPAA risk management plan every year. More and more enforcements are being made for organizations that fail to do a HIPAA risk analysis, and have a risk management plan, as opposed to an actual breach incident. OCR may investigate if they suspect that an event has happened, or a breach has been reported, but more and more they're enforcing and levying fees, and fines, and penalties for the lack of a risk analysis plan.

Jenn Behrens: Going through a risk analysis will also help you walk through your privacy and security controls, and the different contracts vehicles, like a PIA and a QSOA that you may have in place. So all of this is intertwined and is good practice to walk through.

So then at the end of the day, we're still stuck with, well, do we share or do we not share? If you have checked your boxes for your federal regulations that you are operating within the confines of how you can share with HIPAA, that you have a QSOA, or you have patient consent between your Part 2 program to share ... The consent between that patient and the Part 2 program to share with an HIE, and possibly downstream organizations; and you've checked your state regulations box that you are permitted to share this information based on whether you have that consent in place, or you have a QSOA, then this becomes a risk-tolerance exercise.

Some organizations do not want to accept this risk into their systems. And there are valid reasons for this, especially if you're working with organizations that have a lower risk-tolerance for their business. There are a lot of healthcare organizations that just are much more compliant-focused and do not want to accept any level of risk. They don't want to get out ahead of what's going on in technology, and their stakeholders do not welcome that type of risk-tolerance into their program.

Jenn Behrens: Some are more open to accepting some of that risk. I will say, one of the things that comes into play increasingly with this, "To share or not to share?" question is, especially with HIEs, is across state jurisdictions, so especially if you're looking at a patient center data home type of approach, or if you're looking at national HIEs - those larger exchange networks that are happening, and people are onboarding to.

So if you're looking at that, you need to understand not only the risk within your state regarding your own state's legislation; please also consider the risk that you're looking at from that other state, and the exchange that you're going to be invoking between the states and amongst them and the patients that are then bouncing back and forth and the consent mechanism.

You can see how this can get very complicated. I would say if out of all these topics that we discussed here the question of oversharing or not to share, this is probably the dead horse to beat. I would say make sure that your organization has a clear and agreed upon decision for this. This goes beyond checking the boxes over your federal regulations, your state regulations, and then looking at your consent models. This comes down to a business decision that you want to get all your key players and stakeholders on the same page for and moving forward. This is a very complex and complicated matter, and having consistency between your key stakeholders internally as well as your external stakeholders is going to be critical for minimizing any complications for your onboarding participants, and then also making sure you have a consistent approach to managing the care for the patients that are involved in your exchange network.

You also want to consider and understand what your decision will mean for your participant organization. This is what we'll pull out a little bit more in the next webinar. You want to understand if you're asking them to update their consent model. If you want to go back to your Part 2 programs and make sure that they have articulated consent mechanisms between those organizations and the patient that then permit sharing with the HIEs and then are you looking at sharing downstream also in that consent mechanism? There may need to be adjustments to their consent model. Are you asking them to sign extra amendments to your participant agreement? You already have a BAA with all your participants, and now are you asking them to sign a QSOA as well? Consider that there are these types of housekeeping and administrative implications for figuring out how you're going to share or if you're going to share or if you decide you are going to share, then you will have to go through likely a socialization process with your participants and look at if you are going backward or are you just going to go forward? Again, this is when you take a complex matter and make it complicated because you have all these different implications. Again, this can be largely thought of as a risk tolerance exercise because you're also looking at the likelihood of your participants to participate in this type of protocol and exchange.

This can get somewhat tricky but when this starts to seem like it's becoming overwhelming, I would encourage you to go back to what are the simple definitions? Break apart exactly what types of data you're looking at, where they're originating from. This gets to that 42 CFR part 2. Are these really coming from Part 2 programs or not? Then are you really considering the mechanism to contractually enable yourself to get the exchange or are you looking at the protocols that are more security and privacy consent based? Go back to some of the definitions and break apart the types of data and the types of participants that

you're looking at, and then you can start assigning the different types of mechanisms and methods to exchanging that data if you choose. Just again, beat that dead horse. Make sure that organizationally you have a consistent approach to this before someone makes a step to onboard a participant in a certain way or to exchange a certain amount of information as you can go down a rat hole really quickly if you're not sure where you want to land.

That was a lot of information in a relatively short period of time. We are going to have another webinar where I hope to hear a little bit of dialogue from you now about what you're doing currently to manage behavioral health in 42 CFR Part 2 regulated data and then our next webinar is going to pull apart some of what those consent models look like but this conversation may also inform additional topics that we may look to interweave in that next webinar. Sharon, I'd love to open it up and see if there are thoughts and again your organization may be doing this very differently than other organizations. What I can tell you from the research out there right now is there is not one consistent approach that has been deemed better than another. I think this is a good learning exercise and a good healthy exercise for all to have as we look towards hopefully understanding this context of these different types of data more clearly.

Sharon: Thank you very much, Jen. I have opened the line. If you have a question for Jen, please go ahead. Let her know your name and where you're calling from. Phones are off mute. If you have a question, please go ahead.

Melissa: Sharon, this is Melissa. I don't really have a question but more a comment. Jennifer, thank you very much for the presentation. This is Melissa Kotrys with HealthCurrent in Arizona. The comment I would make is I agreed with all of the areas of caution, complexity, etc. We've been down this road over the last at least three years, and really now are identifying a lot of the challenges relating to workflow. We've identified them before, but when you implement these types of regulations it's not just about the technology but a lot of times the workflow and the new consent processes that organizations have to put into place be in compliance. If it's helpful to the future presentations, we're happy to share the framework of how we've structured those. I appreciate your presentation and agree it's a really complex space.

Jenn Behrens: Absolutely. Thank you for that feedback. I think anything that you'd be willing to share would be welcome amongst this group. Certainly I would appreciate learning more about it as well.

Melissa: We'll follow up separately with you offline to share anything that might be helpful.

Jenn Behrens: Okay that sounds great. You touched about the different technological solutions to consent management, which is probably a whole different webinar series, but there in the identity space consent management is really hot, and it's starting to coincide with healthcare organizations and certainly with HIE consent management. There are different approaches to managing consent. There are different varieties of consent management, just between community-wide or participant-wide, provider-based, but then there are also different ways to manage that in your technology solutions, and so you're exactly right. It can be very complicated, and if you add on competing regulations that can get very complex as well. I completely agree.

Melissa: Actually I did think of a question. This is Melissa again if no one else is jumping in. I'm headed to DC tomorrow for health IT week. I've been only loosely following some of the federal regulations. My understanding is, and I guess I'm trying to clarify this with you and see if you have any more concrete information, that the joint package related to the opioid epidemic that was signed by the president, one of the sticking points was the alignment of 42 CFR Part 2 with HIPAA that I've been really hoping would be pushed through, and that was taken out before the legislation was signed, but I've also heard that there still might be other bills floating around that still have that in. Can you confirm whether or not that's true, and/or if there's anything more you can share about federal legislation to better align Part 2 and HIPAA?

Jenn Behrens: So I would say I would not be surprised if there are other amendments or other efforts to align the two. I do know that you're exactly right. The part of the package that would align Part 2 with HIPAA was removed. HHS decided not to push on that one. I don't have any more information other than that was really disappointing. I would be interested to see what you hear when you're in DC and that others on the line have heard as well, or any other information.

Speaker 1: You had mentioned getting in good relations with your attorney general. What is your exact experience with that?

Jenn Behrens: I will say that I've had the unfortunate experience of working with an organization that first got in touch with their state attorney general when there was a breach. It's just much more challenging. When I sometimes work with organizations, I like to reach out to either the attorneys that are guiding the overarching state regulations and that guidance. Often the authors or main attorneys who are influencing state guidance on those regulations or just trying to reach out and contact your state attorneys general and their offices to understand some of the implications of some of your more complicated state regs and how they impact federal. I will also say one of my, and it wasn't on the slide here, but I have contacts at HHS. Sometimes for some of my orgs I just ping them every so often, and I stay in touch with them just to maintain an open communication cycle.

If there's a hypothetical, and I'm doing air quotes that Y'all can't see, but if there's a hypothetical issue that comes up with one of my orgs, then I can go, and I have gone to my contacts at HHS and run through what this might look like. It goes a lot better and a lot more smooth, because it's a lot quicker. They're much more responsive and supportive in how to navigate these issues before they can go sideways. I've done this for healthcare orgs but then also for GLB regulated data too. Just with all those types of data sets too, I would encourage you the more you establish contacts with those sorts of representatives early, the better because again your communication cycles are more efficient, you can tackle some hypothetical. Like if you see something brewing and you just get a feeling, sometimes it's good to reach out to a friend that you have in one of these departments to say hey what do you think about this? Then, if you do need to make a business decision you also have some comfort in knowing that you've already said is this.

I did this recently with one of my HIE orgs, and it was a brilliant move by that ED to get on the phone with one of the attorneys that oversaw state guidance. It just was extremely beneficial, and there's much more comfort in moving forward, and we've been able to

navigate some of the work streams that were just kind of throwing up question marks for all of us. The group was the ED, the account sales, the legal counsel, external legal counsel, me as CSO, and our technical and our project managers. This is where I get into the if you're going to beat a dead horse, this is the decision you need to beat a dead horse on. Walking through with that higher-level guidance just was exceptionally beneficial, and now there's much more confidence in making those decisions moving forward. Also, just informally, I have found that the people in those positions at the state and the federal government are pleased and willing to talk to you when there's not a protocol issue happening. They really welcome that interaction. I've only found them receptive and friendly.

Speaker 1: Thank you. That's helpful.

Sharon: Anyone else have any comments, questions? Well, hearing none, I will go ahead. Again I want to thank Jen for a wonderful presentation. Our second part of this discussion, part two, will be held on October 25th. I want to thank everyone on the line now for attending today. Have a good afternoon, everyone.

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.](http://www.kuma.pro)