Protecting Data in an HMIS Environment Privacy, Security, and Confidentiality

0:00:07 Mike: Okay, good afternoon everyone. My name is Mike Lindsay and I'm with ICF, and I'd like to welcome you today to the first set of remote sessions for the National Human Services Data Consortium, co-sponsored by HUD, HUD's Office of Community Planning and Development. I'd like to welcome you to the NHSDC session entitled "Protecting Data in an HMIS Environment: Privacy, Security and Confidentiality." Again, my name is Mike Lindsay, I'm with ICF, I'll be one of your presenters today, and I'm joined today by Fran Ledger from the Office of Housing and Urban Development. Fran, you wanna go ahead and introduce yourself?

0:00:46 Fran: Hi, I'm excited to be here today and welcome, thank you for joining us. I am with the office of the US Department of Housing and Urban Development. I hope you get a lot out of this presentation today and I look forward to your questions.

0:01:01 Mike: Thanks a lot, Fran, and thanks for joining us today. Also, I'd like to thank Chordiant folks on the back end for helping us out with some of the Adobe Connect. For folks on the call today, if you have any questions, if you have any questions for us, content-related questions or technical questions or just dialogue that you'd like to provide, you can use the chat function. If it's a technology challenge or problem, Chordiant folks are working on our team, will connect directly with you and try to help. If it's content-related question or comment, Fran and I will do our best to address it during today's session, either in writing in the chat or we'll try to address it verbally as well.

0:01:37 Mike: We wanna specifically thank everyone for taking the time to join us today as we're all dealing with the health crisis not only in our personal lives but also in our professional lives, times are tough right now. All of us are being pulled in multiple directions, we have multiple and shifting priorities. We appreciate that you're taking the time to spend with us today. We're excited about the opportunity to talk to you about privacy, about the potential opportunity to revisit, relook at your privacy models, release of information models, etcetera. If not at any point, in the implementation of your HMIS systems, your coordinated entry systems, but probably, specifically right now, with the challenges that folks and communities are dealing with.

0:02:20 Mike: So again, if you have any questions or comments, please feel free to drop your question or comments in the chat, and then to follow Miranda's lead, feel free to say hello in the chat. We always appreciate hearing from folks, knowing who's on the line, as well as what CoC you represent. Helpful for Fran and I to know what parts of the country are joining us today. So feel free to use that chat function and we will do our best to get back to you as questions and comments come in.

0:02:48 Mike: So just a couple of quick words about NHSDC. So again, when Fran and I started to think about this session six months or so ago, we never imagined that you'd be joining me in my home office. We thought we'd be sitting somewhere with you in Minneapolis, having an opportunity to have a very interactive dialogue around a sophisticated, complicated concept like privacy, data sharing, etcetera. We don't have that luxury today. We're gonna do our best to create an environment here where we can address questions and we can talk through things.

0:03:18 Mike: But just very quickly, for folks who have had the opportunity to join us, other facilitators at NHSDC in the past, NHSDC is an organization that's focused on bringing HMIS data and technical experts together to advance the field of homeless services through the lens of stronger data, stronger data systems, and advanced data users.

0:03:41 Mike: NHSDC offers opportunity for community members to provide information, to gain assistance or to engage in peer-to-peer education and lifelong learning opportunities. NHSDC historically holds two conferences annually to create this space for us, for folks like you in the field, and the last three events have been co-sponsored by HUD and we're expecting that to continue moving forward. So we're all disappointed that we're not able to engage together today, but we're really excited about the content of today's session. So just real quickly, to go through our learning objectives today so folks have a pretty good sense of what we're hoping to cover. Fran and I hope to identify with you today, strategies to better manage your data in an HMIS environment that meet the needs of clients, projects, and the system, while protecting and respecting client choice regarding how their personal information is managed.

0:04:35 Mike: Now I wanna just hit on one point in this first objective for a second, we're defining an HMIS environment. And I think as Fran and I discuss with you today, different options that you have regarding privacy, privacy postings, release of information, it is looking at the entire HMIS environment. So you'll hear us talk about data collecting, your HMIS system, as well as data that is used in your overall coordinated entry processes, procedures, whether or not it's collecting your HMIS system or not. So we'll be very, very clear to pull out those points throughout today's session.

0:05:13 Mike: We also wanna spend some time helping you to clearly understand and discuss the key roles, the key rules, regulations and fundamentals around data privacy and security, to help to understand the fundamentals of the required and permitted uses and disclosures of personally identifying information. Really understanding the difference between uses and disclosures, how they interact within your HMIS system, but more specifically, how they interact with your privacy policy, privacy posting, and release of information if necessary in your community. And then very specifically through the lens of today's session, we wanna review and discuss common privacy barriers or challenges for utilizing or leveraging your HMIS system in your coordinated entry systems and environments.

0:06:03 Mike: So before we jump into some of the grittier details today, the first two slides we're gonna take a look at or slides that we, HUD, NTA providers, specifically through NHSDC, have been using for the last couple of years. And I think when we started to use this slide, we were really talking to folks like you, folks in communities, to get communities to think about things in a different way. After the HEARTH Act was released, we saw very clearly HUD's move towards moving away from program-by-program, client-by-client decisions, moving towards a system performance system management. This is how we started to get communities to really break that mold of how services were provided in the past and to start to think about how to better coordinate services in your community.

0:06:51 Mike: I think it's valuable now to bring us back to this type of concept. Not because you guys are still at this place. Most communities have coordinated entry systems, and we'll look at a diagram of one in the moment, but some of these systems are functioning at pretty sophisticated and high levels. What we'd like you to do today is think about this shift from program by program models, think about shifting away from, continuing to shift away from unique agency intake processes, haphazard decision-making or just housing the next person in line.

0:07:24 Mike: When you're thinking about how... So, that's how systems used to operate. If you're thinking about how your system operates today, hopefully it operates in a more coordinated way. It

operates with a defined coordinated entry process, you are making data-driven decisions for how your programs are funded, how clients receive services in your community, but also how to prioritize folks in your services. As we're thinking about that at this point in time, Fran and I wanna talk with you today regarding the opportunities, challenges and the potential of revisiting your privacy policy now to benefit your community during the health crisis and position your community strategically to be more client-centered and more efficient and effective moving forward.

0:08:07 Mike: So, as we're thinking about this shift, we wanna think about this shift from the perspective of where your community is today. But when we look at a sophisticated coordinated entry model like we have up on the screen today, think about how clients cycle through your system, how they may come into your system, access your system. They may be diverted out of your system, they could be receive targeted prevention services. They might need emergency shelter for that. They might cycle back out of your system, back into your system.

0:08:40 Mike: We start to think about your different access points, different models of assessments, different progressive assessment models, different prioritization processes, start to really identify in the community how many different touch points there are for every individual or family that accesses your system, not only how many touch points there are, how many times that data is collected from them, how many times it's explained to them, how many times it's re-collected from them. And when we're looking at these complex models, we know a lot of communities have existing privacy policies that they may have taken from another community built off of the best practice but may not have been designed in a way that was going to give the community the most efficient process for the participants accessing services in your community.

0:09:30 Mike: So, if we're thinking about this process, thinking about this structure, what we wanted you to think about today is regardless whether you look as sophisticated this model or as unsophisticated this model looks, depending on your community, I really want you to think about how you're currently collecting data, how you're... If you're requiring a release of information, how it's applied, where it's applied, and if it is truly client-centered, if it creates any barriers to your system. What we wanna talk to you today is the options that you have available through the privacy model, through your privacy policy, privacy model release of information as well, really make your systems as client-centered as possible, protecting client-level information all the way through the system, but creating efficiencies within the system so that clients are connected to services as quickly as possible.

0:10:25 Mike: They have to retell their stories as minimal times as possible, data is collected where it needs to be collected and to be shared with folks that are coordinating services around those individuals. Multiple ways that it can be done in multiple communities. What we wanna talk about today is how you should be considering this right now and having folks reconsider their systems, reconsider their privacy policies and being very clear around the requirements for both.

0:11:00 Mike: Okay. So, what about data privacy? So, CoCs need to thoughtfully approach how date is collected, used, stored and, in some cases, how it's disclosed across your homeless response system. Service and housing decisions are based on sensitive participant information that's collected over time from multiple individuals and potentially used by multiple providers in electronic and printed formats. So, I think that's important. I wanna plug that here. Electronic and printed formats. We're gonna touch on that concept a couple of times throughout today's session. The privacy and security is made more complex by multiple rules, multiple regulations that exist across federal

partners and federal states.

0:11:41 Mike: So, it's important for CoCs and providers to make informed policies and procedures and fully understand the following: How data is collected in your community, how it's used, where you store it, how you store it, how it's, and most specifically for today, how it's disclosed, if it is disclosed, across your community. Ultimately, how clients understand how their data will be used after they provide their data, after they accept services. Yeah, so that there's a client-centered approach to why data is collected, how it's collected, and then how it's shared, who it's shared with, and how their services are better informed by that. Really understand the responsibility to collect, to protect client information and be able to articulate these responsibilities to clients in a meaningful way.

0:12:30 Mike: In communities that we've worked in in the recent past to untangle their current privacy policy, what communities thought was a client-centered approach, a lot of times when we have them take a look at it and really look at how the release of information is applied in their community, how their privacy policy is applied in their community, a lot of communities start to see that the system that they thought was client-centered, thought protected client's information, maybe didn't as intentionally as they expected it to. And regardless whether it changes necessary revisiting the process, revisiting the scope, training folks on how to apply the model in general is critical for any communities even if your community decides, at this time, your privacy policy does meet your needs and adjustments that are available to you today have been available to you in the past aren't necessary at this point.

0:13:25 Mike: So, coordinated entry in HMIS. HMIS is obviously not required for coordinated entry, so HUD doesn't require, HUD does require you to have an operational coordinated entry system in place, clear policies and procedures, etcetera, they don't require you to leverage HMIS or to use your HMIS system in your coordinated entry system. What we've seen in most communities that we work in, is to have an efficient coordinated entry system, utilizing HMIS is critical in that process and data sharing across providers is also a critical part of the process or an opportunity that communities should consider.

0:14:04 Mike: So there are a lot of benefits in utilizing or leveraging your HMIS systems to support your systems of care, specifically your coordinated entry systems. They could be used to easily identify available units. So if you collect your information in HMIS, if you're considering or currently making online referrals through your HMIS system, your HMIS system can be used for the referrals, and could also be used to identify capacity within your system so that you know, as you're making referrals, they're being made to an open bed for an open opportunity.

0:14:38 Mike: You can use HMIS to track client progress, from the assessment all the way through enrollment. It can be used to help facilitate the coordination of care, either through case conferencing, through your referral process, etcetera. It can absolutely improve data quality. We know how to manage data, if we know how to manage data quality in an HMIS system, how to set appropriate benchmarks, how to set appropriate action plans, to increase those outcomes, etcetera. So the more data that's collected in our systems, in your systems, the more the security of your system can be emphasized for those processes as well as data quality policies, procedures that you have in place, privacy and security procedures, as well.

0:15:22 Mike: Ultimately, and we should be ever more aware of this during this period in time, but

it reduces the trauma on the client. The least amount of time they are asked the same questions, they have to give the same responses to different folks, the more times they have to tell their story, requires those individuals to revisit aspects of that trauma that may not be healthy or beneficial to them at this point.

0:15:50 Mike: But regardless if HMIS is used to support your coordinated entry system, a couple of very critical issues still apply. So, again, regardless whether you use HMIS for coordinated entry, or not. So if you use paper forms, if you use some type of other technology, there's a couple of points that still apply regardless. So your HMIS privacy and security policy developed by your community, approved by your CoC, still apply to data collected through your system, to support coordinated entry whether it's collected in your HMIS system or outside of your HMIS system. We will dig more into that in more detail in a handful of slides.

0:16:30 Mike: There also has to be written policies and procedures that define how consent is obtained, documented and how client data is shared. Clarity that clients are not denied service if consent or data is not provided if it's not required by the funder, federal funding source and all HMIS end users understand the privacy rules related to collection, management and reporting of client data. I'm gonna go one step further on, on the last point. I would say that it's not only that your HMIS users understand the privacy rules, it's that they have the tools and resources to be able to articulate it in a meaningful way to any client that they're collecting data from, anyone that they're interacting with, collecting data and putting into the HMIS system, being able to clearly articulate the need, the goals and the process for clients as they are accessing the services is critical in all communities in every interaction.

0:17:29 Mike: Real quickly, I wanna touch on a couple of the... A couple and then a lot of the regulations that need to be considered as you are thinking this through. So as...

[pause]

0:17:45 Mike: CoC's data management...

[pause]

0:18:05 Mike: System is used to record information about coordinated entry process, must meet the following HUD requirements. Coordinated entry requirement, coordinated entry notice, as well as HUD's HMIS privacy and security notice. All of these you're, I'm going to... We're going to assume relatively familiar with. I think part of what's coming back out through our discussion today, goes back to the HUD's HMIS privacy and security notice and standards that came out in 2004. Some of the data... Some of the concepts that we're going over today have been in existence since 2004, there's been a lot that's happened in the field. A lot that has shifted, a lot of best practices that have come out and some of those core policies responsibilities, opportunities from 2004 have been, I won't say lost, but through the establishment of one Privacy Policy in the community being leveraged in another community, some of those concepts we see, need to be revisited, or re-understood by communities.

0:19:07 Mike: So that's the majority and part of our goal for today. Spend real quick moment. So on this slide, probably one of our denser slides for obvious purposes, identifies the key rules, regulations and privacy fundamentals that need to be considered in your communities, as you're

thinking through your privacy policy, release information policy. There are HUD HMIS data and technical standards, Health Insurance Portability and Accountability Act, folks, I'm sure are very familiar with the concept of HIPAA. We're gonna say a little bit more about that. As well as part two VAWA, VOCA, and then at the bottom, your state and local privacy laws. That's a critical point. So every state has different privacy laws, some have a pretty large impact on what you can do locally versus HUD guidance.

0:20:03 Mike: Some are a little bit easier to deal with. We certainly recommend before you look at your privacy policy, before you start to consider making an adjustment, get some legal advice, some legal counsel to better understand any local or state privacy laws that you will need to comply with, and make sure that we're clear, you're clear on how those interact with your other federal requirements.

0:20:26 Mike: There's just a couple things I wanna point out here, just as by way of reminder, or level setting, or just bringing everyone to the same level of understanding. When we're thinking about these rules or regulations, it's important to remember that just having health information about a client does not mean you're covered by HIPAA. So your organization, you as an individual, or your HMIS system, just having health-related information in there doesn't necessarily make you a HIPAA-covered entity. And similar with CFR, or 42 CFR Part 2, having drug and alcohol information about a client doesn't mean you're necessarily covered by Part 2, as well. So it is thinking about how these are applied, if they're applied to your organization and in your community.

0:21:11 Mike: Just one quick note about domestic violence, the Violence Against Women Act, VAWA and the Violence, the Family Violence Prevention and Services Act, you'll see that acronym, FVPSA, and the Victims of Crime Act of 1984 regulations prohibit sharing personally identifying information about victims without informed, written, reasonably time-limiting consent. Both VAWA and VOCA also prohibit disclosure of individual information without consent. So this clearly makes it, prohibits programs from making the signing of that type of release of information that condition on services. But if that's applicable in your community, certainly recommend that you take a look at it, understand who's covered by it, understand how that works within your HMIS system and your coordinated entry system, and if you have questions or challenges, you can definitely request TA, TA around that.

0:22:10 Mike: But just a couple of examples. I wanna talk very briefly and then we're going to move on to some of the more specific content for today. But just a couple of examples where providers must comply with the requirements that provide the greatest protection for the individuals, PII. So again, the federal requirements are set, unless a stricter requirement, either local or federal, applies in your community. But just a quick example of how this works.

0:22:39 Mike: So a provider may be obligated to meet the Health Insurance Portability and Accountability Act, HIPAA, privacy and security requirements because they are a covered entity. If so, this provider will follow the HIPAA set of privacy standards, not the HMIS privacy standards. But most times, service providers are not covered entities. Health information, for example, about a disability shared by an individual directly with your 211 agency, directly with your access point, is not necessarily subject to HIPAA in the hands of the agency. An agency not subject to HIPAA otherwise does not become subject to HIPAA just because it receives health information from an individual or from a HIPAA-covered entity.

0:23:24 Mike: A lot of communities, as we start to pull apart and untangle privacy policies, what communities have available to them, there's a lack of understanding for when HIPAA applies and under what circumstances it applies. If you have questions, further questions about that, certainly you can drop them in the chat, you can request TA, or to use the AAQ system at any point to gather some of that information.

0:23:52 Mike: A couple more concepts about victims with implications for victim service providers, and then we're going to go ahead and move on. But the domestic violence providers, again, prohibited from entering personally identifying information into your HMIS system, and must use a comparable database. Comparable databases have been a topic of conversation for a long time for at this point in time a comparable database. So a system, in order to be comparable to HMIS, it has to have the capacity to support HUD privacy and security requirements, and at a minimum, meet the data standards requirements and produce HUD required reporting files. So if you look at the data standards, the data manuals, etcetera, reports that need to come out of HMIS systems, essentially comparable databases need to be able to meet the same goals, collect the same data in the same ways, report the same reports.

0:24:48 Mike: Victims of domestic violence must have access to your coordinated entry system. There are a couple best practices out there for how communities have started to establish this. This is certainly an area where communities need to be flexible, need to think outside the box a little bit within the constraints of what's legal, but look for ways to be able to better incorporate those programs into your coordinated entry system, as well as those individuals and families so that they have just as equal and fair access to the services available in your community.

0:25:22 Mike: So with that, I'm going to turn it over to Fran to talk a little bit more about the grittier details of data privacy requirements. Fran.

0:25:29 Fran: So what I wanna do is I'm actually gonna take just a break for a minute so we can answer some questions that came in, and then we'll move on to my section. But I think that it's one of the questions that came up was, "What do we do around coordinating care when a client refuses to sign consent?" And I think that we... The client always has the right to refuse to share data. So, I don't know, Mike, can you talk a little bit about what your experience has been with working with communities where you're addressing issues around client disclosure and the sense of choices that clients have around that?

0:26:24 Mike: Yeah, can you rephrase just a tiny bit of that question? I was reading the [0:26:27] ____ question.

0:26:30 Fran: Sure, the question is around, how do you take the coordinating part of it? So what happens between the providers and your coordinated entry process when a client refuses to consent to share information between the providers?

0:26:48 Mike: Yeah, that's a great question, thanks Fran. I think there's a handful of ways that that can be dealt with and that can be addressed and I think part of it, we're gonna talk through some of it here today. So, that consent part for the coordination of services doesn't necessarily need to be gathered through your privacy policy. So we're gonna talk a little bit... We're gonna talk more about that in detail, in a moment, but I think some of the opportunities in that question are probably reflective also in the conversation we had right before we started this dialogue here.

0:27:22 Mike: And that's better thinking how to include victims of domestic violence or domestic violence providers into your coordinated entry system. That information can't be shared, can't be put in their HMIS systems as well. So I think a lot of communities are creating other aliases or they're creating codes that they're using, and then they're sharing that level of information only potentially a little bit of additional information with their coordinated entry systems so that those individuals, even if they're not being identified in any way, their situation would be prioritized. They could be prioritized within a single prioritized list and they can gain access to a service.

0:28:04 Mike: It takes more of a human-human interaction, so if when that individual or a family is potentially ready to be referred, it gotta be connection back to that organization to identify who they are, how they can get access to the service and how that connection needs to be made. So I don't think there are simple solutions there, but I think there are solutions that communities are working through. Some of the domestic violence, VAWA provided or VAWA solutions that communities are coming up with in communities, I think could be applied in very similar ways to clients who do not choose to have their data shared for the purposes of coordinating services in their community.

0:28:47 Fran: Yeah, that was great. And as you have more questions that come up, go ahead and say back. And so we have a couple of questions that have popped up around HIPAA and I just wanna be clear that so... And probably many of you know this. So, HUD does not have statutory authority over HIPAA. So we're providing some information regarding HIPAA but for clarification around HIPAA, you really wanna go to Health and Human Services that oversees HIPAA statutory language. But know that the HMIS data and technical standards, the privacy portion is based on HIPAA standards, however... And HIPAA is not... It's actually not very stringent. And so I think that it's not a factor of it being a really complex thing, and also know that most homeless service providers aren't actually a covered entity under HIPAA. Very few organizations are a covered entity or would be a business associate under HIPAA.

0:30:04 Fran: It's really limited to healthcare providers, so those that are like a hospital, doctors, pharmacies, those type of organizations, organizations that operate health plans and healthcare clearinghouses. Those are the types of work organizations that you find are under, they're covered entities. But some of the same policies that you see under HIPAA are the same policies that HUD has adopted for making sure that we're protecting client information. But we'll look at the questions that you've posted around HIPAA and we'll answer more questions about that, and I'll go ahead and keep going on the presentation. Michael take a look at the questions and drop those into the chat.

0:30:58 Fran: Okay, as the HUD representative on the line, I'm going to talk about HUD's requirements this portion. So this is... So we'll move away from HIPAA, we'll talk about HUD's requirements for this. So yeah, so we have a baseline privacy requirements. They date back to 2004 and with Coordinated Entry, we've been very careful to get more clear about what the privacy requirements are so folks can be more thoughtful about the privacy requirements, and go back and relook at them. Mike described that a little bit.

0:31:40 Fran: And so, this slide here is helping talk about some of the primary things that need to exist. And one of them is you need to cover your privacy policies in your coordinated entry policy and procedures. And so that privacy policy covers kind of your... Everything that encompasses how you are gonna address your privacy standards. So that is one way in how you communicate out what your policies are. The other is the privacy notice. And the privacy notice is really a summary

of what your policy is. And in your privacy notice, this is something that you can hand to participants and it includes things like what are the right... What are the participant's options? What is the responsibility that you are taking on as an organization to protect personally identifiable information? How is information getting used and disclosed? So all those basic things are in your privacy notice.

0:32:45 Fran: The other thing that needs to be listed in there is how you manage a breach if a breach occurs. And know that HUD doesn't prescribe to you how you manage a breach, it just states that you have to have a process for handling a breach. However, there might be other federal, state, or local laws that do dictate how you should manage a breach for your community. So you wanna be careful about what those might be and and how you incorporate that into your policies.

0:33:17 Fran: You also have to have a grievance process. So you wanna think through what that looks like. And when we do receive through our Ask a Question, occasionally, we'll receive something from communities around a grievance from participants around how information is handled. And so you need to have locally a grievance process so a participant can come forward and say, "I don't like how my information was handled. I think something happened in a way that was inappropriate or not how I understood it was gonna be handled." And so you have a process for how you manage the grievance. And staff need to understand what that grievance process is so if a participant comes to them, they're able to describe what that is and help that person connect with whatever the grievance process is. That's really important.

0:34:10 Fran: What's really good to know about your privacy notice is that the privacy notice can be amended. And the privacy notice, when it's amended, is retroactive. So you wanna take a look at that privacy notice on a regular basis to make sure that it's really reflecting the structure that you need to have in place to be able to be successful with coordinated entry and that you're doing the things that you need to do to take care of the stewardship that you have over this information. And so if the notice is, there are issues with the notice and that it needs to be adjusted, that could happen.

0:34:55 Fran: There are some parameters around that that you have to be careful about. You cannot make it... You cannot adjust it in a way that removes the HUD requirements, those baseline requirements absolutely have to remain in there. So be careful of that. And you wanna make sure, again, if there's any federal, state, or local laws that you need to consider, that those remain in your privacy notice. And we always encourage communities to think about having someone who has some legal knowledge around what those things are for your community, to take a look at that and give you some feedback on that when you go to reevaluate your privacy notice and make changes if you're feeling like that's necessary.

0:35:47 Fran: One of the other things that's really important around data collection is that you have a public statement. You want it to be transparent about what you're doing, and so one of the things that's in the 2004 Data and Technical Standards is that you have a public statement and it should be available for people so they know how that information is being handled. And we put an example statement out. It doesn't have to look like this, but it does need to have all these elements in it. So it explains how their information is being handled and that they can get access to the summary of the privacy policy, the privacy notice, so they know how to get a hold of that.

0:36:30 Fran: And I think with people doing things like street outreach where they may not have an actual physical office, where people are meeting participants in person, there's a variety of ways

that this can be handled. It could be on a clipboard, it could be read to somebody over the phone, but you need to make sure that there's a way that individuals are being informed on what's happening to their information that you're collecting.

0:37:14 Fran: A part of your notice is gonna include several pieces. There are things that we describe as, around uses and disclosures that are required, permitted, and prohibited. So I'm gonna talk a little bit about what is a use, what is a disclosure, and then what are these three buckets. It's helpful to have these things separated out and understood 'cause it helps us understand how we handle information when we want to figure out what's appropriate, what's not appropriate for when we share this information, or we determine that we can't share this information.

0:37:57 Fran: So when we're thinking about uses, we're talking about those things that we do, those internal activities. How do we actually use this information. So it can be how we make decisions, so that might be a use. How we use it maybe for internal monitoring or something along that nature. So what is the internal activity for which the provider is interacting with that information that's been collected?

0:38:26 Fran: The disclosure is what happens when we then share that information out beyond that entity, so we're sharing it to a third party. And then for uses and disclosures, we talk about three things. We talk about those things that are required, those things that are permitted, and those things that are prohibited. So you heard Mike a little while ago describe a bunch of different laws, and several of them had provisions. So we talked about VAWA that had restrictions around how information could be used and disclosed. There are other ones.

0:39:03 Fran: So those are ways in which there are strict guidelines around what you cannot do with data. In the 2004 Data and Technical Standards, there are many permitted uses. So HUD says that these things you are allowed to disclose information in these particular ways, and we're gonna go over those in a few minutes. And there are two required things that you have to do if you were asked you need to provide a copy of the record to the client. So if the client asked, "I wanna see my records," then you need to provide them with the records, so you need to let them see it. So these are the kind of buckets that we need to think about when we're thinking about uses and disclosures.

0:40:00 Fran: So this slide here talks about the different authorities that HUD provides communities with around disclosing information. So HUD kind of separated these out into two pieces but they don't really need to be. It's really a long list of permitted uses. So these are the first four that we describe and this is around coordinating services, this is the big one, this is the one that's really tied in with your coordinated entry. So this is when we talk about communities about disclosing information to multiple coordinated entry providers, it falls under this bucket, this is a permitted use. And this is to connect individuals with appropriate resources and services.

0:40:49 Fran: We also have creating the identified client records for PII. This is around making sure that you are able to make sure that you are clicking that information and that you are actually been able to report out on your record. So this is also a really important use piece. And then carrying out administrative functions. So, these are legal audits oversight in this bucket, this allows for system administrators to have access to all of this information, it falls under this piece. And then the functions related to payments and reimbursements.

0:41:34 Fran: So all of these are permitted and then we have these other pieces of uses and

disclosures, those required by law, those to avert serious threat in health to safety, uses and disclosures about victims of abuse, neglect or domestic violence, those for research purposes and those for law enforcement purposes. It's important to note, extremely important to note that if something is not in your notice, so all these things you'll wanna have listed in your notice as permitted uses and disclosures, if it is not in your notice, then you need to obtain consent to be able to use and disclose this information. So this is the key piece. As you go back and look at this privacy notice, you wanna make sure that they're in there. If they're not in there that may be something you wanna then do an amendment around.

0:42:39 Fran: One of the two things I wanted to point out that I think is really important right now, are those uses around those being required by law, and those to avert serious threat to Health and Safety. So let's talk about those for just a second. The one around using and disclosing when required by law. So this is really to the extent that the use and disclosure complies with and is limited to the requirement of the law. So you wanna make sure that when you're being asked to disclose information by a legal entity, that it's limited to whatever that request is, and we'll talk a little bit about what that looks like in just a minute.

0:43:27 Fran: And then for those that are disclosures that happen under the serious threat to health and safety, you really... That there's two key things here that the provider that's doing that disclosure needs to have good basis and believe that this will actually avert a threat to health and safety, and that the person that receives it, the entity that receives it, can actually do something about it that can reasonably prevent or lessen the threat. If that does not exist, then that's not a reasonable situation to be disclosing information. So keep those things in mind. I think that's helpful.

0:44:14 Fran: So, authority to disclose is not unlimited. When I just described the legal piece to and about disclosing it, know that it's... If a legal entity or a public health agency is not seeking out or requiring a PPI, or a PII, then you shouldn't disclose it. Limit down the disclosures to what is actually being asked and be careful not to over-disclose. Sometimes a request will come in and too much will get disclosed. Ask questions, what do you actually need? And can you disclose less and still be able to meet the same objective. So try to reduce down disclosures as much as possible. If it is sufficient to give adequate information to provider without disclosing the PPI, for one or more participants, then do so. It's proper not to disclose that PPI. And then do not send a list of all participants to a provider if only one individual is being referred or a subset of individuals. So again, trying to limit down the disclosure as much as possible, that's most important.

0:45:38 Fran: We get a lot of questions coming into the AAQ regarding consent. So HUD does not prescribe what consent looks like. We just say that if something is not in your privacy notice, that you have not said that it is a permitted way in which you can use and disclose the information, then you need consent to do so. So that consent could happen through... It could be written, it could be verbal. It is up to the community and what makes sense to the community.

0:46:16 Fran: But I do wanna have this slide up here so you are aware. Commonly CoCs use forms, and we call them Releases of Information in which to gain consent. Usually those are written consent forms. But again, that is up to the community to decide if that's the route that you wanna go. But you do need to have some form of consent, some form, some way of documenting that you have obtained consent if it's something that's not already in your notice.

0:47:00 Fran: Why don't we take a break for a minute. Mike, do we have questions that we wanna

try to address?

0:47:06 Mike: Yeah, we had a couple questions come in, and also want to acknowledge William Snow has joined, so William's been addressing a couple questions in the chat. Thanks a lot, William. Folks should certainly consider those final responses. So we did have a couple questions come in over the last couple minutes and maybe we... Maybe worth spending some time on, Fran. So we had a question that came in a little while ago from Melissa Nickel, and there were some back and forth in the chat about it, but asking or clarifying that privacy notices need to be displayed at intake sites, agreeing with that, and then asking for options or how to display privacy notices during street outreach engagement.

0:47:49 Mike: So there was some conversation about providing, running a hard copy to individuals being encountered on the streets. There were some comments about hard copies being available on the back of clipboards. We know that folks use iPads at times to have folks review that information, meminated codes, etcetera. That might run the gamut of opportunities there, but wanted to check with you and see if you had anything, any other suggestions for folks. And then we have a couple more questions.

0:48:15 Fran: Yeah, those are the ones I generally hear also. No, I think those are great. Above all, you want participants to understand what's going on with their information and have an opportunity to say... To be able to respond to that. It's the most powerful thing that you can do as a participant, I think, is to actually be able to talk to them about what's happening, make sure that they understand and have that conversation. I think it's really important. And so if it means sticking something on the back of a clipboard and starting that conversation, that works. However you need to do it. We don't have a requirement on that, other than to say that you do need to have some kind of statement in which you are clear to the participant on how you handle that information, and you have to have that privacy notice that's made available to them.

0:49:18 Mike: Okay, great. Thanks Fran. So another quick question came in from Wayne asking about a statement I think I made, a statement about not requiring an HMIS use for coordinated entry. Can you clarify that point? And then specifically through the lens of the coordinated entry data elements being required later this year.

0:49:41 Fran: So if you have a coordinated entry SSO project, you have to use HMIS. You are gonna have to produce an APR. That's what the coordinated entry data elements are for. There is some information up on the HUD exchange that explains, there's a lot of information up on the HUD exchange that describes, that is a... Would be a very lengthy conversation to go through right now. But the information's up there. So if you have a coordinated entry SSO project, you do need to be using HMIS. You are gonna produce an APR. It does need to describe what's going on for your coordinated entry system. However, the requirements for coordinated entry is that you have a data entry system and that it be compliant with the HMIS data and technical standards. It does not require you to use HMIS. So that's the catch. Some communities don't have a coordinated entry SSO project, and so if they didn't have a coordinated entry SSO project, they would not be required to use HMIS. They could use an alternative system.

0:50:56 Mike: Okay. Thanks, Fran. If you wanna take a couple more questions, there are a couple more that we can address quickly, maybe not quickly. A couple of these possibly. So Daniel had a question regarding HIPAA compliance in a data warehousing environment. I think Daniel's question

boils down to, if an HMIS system is going to be integrating data into a data warehouse, some form of data warehouse. That does include Medicare, Medicaid data in the data warehouse. Does the HMIS need to abide by HIPAA requirements?

0:51:40 Fran: The HMIS itself does not need to be... The HMIS is not HIPAA-compliant. It's the providers and the providers are not covered entities. So you really wanna be thinking back to the providers, are they a covered entity and what are they doing if they are to be HIPAA compliant? But if you... This is for anybody that's on the call, you can absolutely submit a question to the AAQ if you have something that you feel like you want to get more specific guidance on and we'd be happy to look at it more in-depth and give you back some more information. But generally, no, your HMIS would not need to be HIPAA compliant, it's your providers that you need to think about being HIPAA compliant if they're a covered entity.

0:52:33 Mike: Fran, last question and maybe we'll wrap up the Q&A finish out and then take a couple of other questions. Does the CoC's privacy notice or client release information need to specify the agencies with whom the data will be shared?

0:52:51 Fran: That's not a requirement in the standards, but it's a good best practice. There needs to be agreements between the organizations on roles and responsibilities, but it's not a requirement.

0:53:11 Mike: Okay. Fran, we can go ahead and talk through how this actually works in reality and then we can take a couple of questions from folks then we can start to wrap up.

0:53:23 Fran: Excellent.

0:53:24 Mike: Okay, so real quickly, we're down to under 10 minutes, about seven minutes left. We wanna spend a little bit of time talking through... At a real high level, have communities done this? Have communities went through this process where they relooked at their privacy policy, privacy notice, release information, relooked at it, re-identified whether it needed... Whether it met the community's needs, revisited HUD's current guidance, revisited the guidance that came out coordinated entry data maintenance guide, as well as some of the COVID guidance that came out most recently, or are there communities that have went through this process and we've seen a couple of communities go through a really deliberate process to rethink, re-understand their need for privacy, their need for privacy policy and release information.

0:54:12 Mike: We're gonna talk through some of that process with you guys here today. So there are some CoCs that have reviewed the guidance provided by HUD and made changes to their privacy policies that allow them to no longer require an HMIS release of information to use in disclosed client information. Very similar to the ways that Fran just described. The communities that have been successful in doing this, have gone through a pretty rigorous process that includes a lot of steps. Conversation started in these communities between the CoC and the HMIS leads in the very early process, and it led to a common understanding of the guidance. So, really understanding what the laws say, what HUD's guidance said, and understanding what opportunities in the community are. Understanding how the current process is.

0:55:00 Mike: This was specific to the community that went through it. So we're certainly not applying this to all communities. But these communities that went through this process they started to understand how the current process they were using that had a HMIS release of information in

place may not have been truly client-centered and actually may have impeded the community's progress to successfully serve some of these clients... To serve individuals and families in their community. It helped them to determine which stakeholders needed to be involved in the conversation about a potential shift in their privacy policy or if nothing else, a better understanding for why the Privacy Policy was established in the way that it was.

0:55:40 Mike: They anticipated questions, concerns, and they also anticipated hold-outs or pushback. So the CoCs that would have went through this process facilitated a community-based process and discussion about the current or potential shift into various stakeholders. So they held meetings with their CoC leadership, and their board members as well as their HMIS leads, participating organizations in their community, as well as their privacy SMEs within the organizations and their HIPAA-covered entities.

0:56:07 Mike: So, just in today's conversation, we can see how complicated any questions revolving around HIPAA compliance, HIPAA-covered entities become. So it's critical for those organizations, those community members to be part of your dialogue as well. End users, intake workers and ultimately hold focus groups with the individuals that access your service and understand how privacy works for them in your communities. The privacy policy and other HMIS documents were then updated to include the move away... Their desire to move away from the release of information and in some communities, this shift has included a move away from both release of information for HMIS as well as coordinated entry.

0:56:51 Mike: That doesn't mean... In these communities, that means that they re-looked at their process, redefined their privacy policy, redefined their notice, as well as retrained all their organizations, all their HMIS end users and their intake workers to fully understand a client-centered approach to privacy, data sharing, consent. Train folks, and put in place a very clear process for how this would be applied at every intake site, every access point, etcetera.

0:57:24 Mike: So, Fran, with that, we have a couple takeaways that folks can think about moving forward. I think as you think about the example that we just talked through, communities that have went through this, being transparent, being informed, having an understanding and then having a community-based discussion around current privacy policy potential to update, potential to consider a different privacy model have that be a community-based discussion, as well as a community-based understanding about the laws, regulations, your flexibility. So, Fran, do we have any other questions that we wanna take today?

0:58:06 Fran: I just, I posted up there just for everyone to see that... Ultimately, remember that the CoC has authority and responsibility for the HMIS. And as a result, when you're thinking about issues over ownership and access, if this needs to go back to the CoC to help make these determinations and around HMIS governance policies agreements, all these things tie back to the CoC. Mike talked a lot today about process and stuff, so keep that in mind. Ultimately, the client owns their data, but the CoC becomes stewards of that information. And the reality is, once information is disclosed, it cannot be un-disclosed. We have to be very careful and thoughtful about what we're doing. And it's really important for the community to think about how they're setting up their privacy policies and how they're conveying that information to the folks that are using the HMIS and the participants who are providing their information that's going into the HMIS. I'm not sure of other questions that came up. Let me take a look here. We only have one minute left.

0:59:45 Mike: We do. Folks have any last minute questions? If you can get them in there in the next minute and a half, Fran and I will be happy to answer as many as we can.

1:00:01 Fran: I would say that probably a really great place to go for information right now around the privacy information that you heard today, is in the coordinated entry management and data guide and that has the most recent privacy information and kind of thinking from HUD's perspective about how to really implement these changes for your community. And we'll go ahead and throw up the link.

1:00:28 Mike: Yeah, and the communities that were used to inform that very brief case study, worked very closely, aligned to the data management guide that Fran just talked about. So Jen Hu asked a question. I think the communities that went through that process used that data management guide. The resources that were in that to inform that community process. So there's a lot of valuable information in there that folks can use.

[pause]

1:01:13 Mike: Fran, we are just about at time. So is there...