OeHI
Office of eHealth Innovation

Meeting Name: Consent Management Workgroup
Call In: Zoom Link: https://us02web.zoom.us/j/84144212711 (Panelists, please use your individual links sent to your email)
Meeting Materials: • Discussion Questions

Meeting Date: 4/18/25	**Meeting Time**: 10:00am-11:30am

Agenda Topic	**Time**
Workgroup Introductions *Allie McGee & Tiffany Sailler* **Members Present:** Allie McGee, Tiffany Sailler, Bianca Melancon, Stephanie Pugliese, Jane Wilson, Katie Nelson, Roberta Lopez, Mary Beth Haugens, John Green, Joy Hart, Lael Crahan, Alexis Harper, Karen Haneke	5-10 mins
Legal and Regulatory Overview *EMI Advisors (Savanah Mueller, Evelyn Gallego)* **Savanah Mueller:** We are here to present the legal regulatory and scope assessments. I'm really excited about all of you that are here on the call, eager to hear some of your feedback and thoughts. Our agenda today is as follows, we'll do some brief introductions, noting who the presenters are today, and then set the stage with some background. We'll be focusing on what consent is, various consent models, and really lay the groundwork for our discussion today. Then, we'll give a bird's eye view of various Federal and State policies and regulations that will play a role in the development of the Consent Repository. We'll review best practices based on insight from these laws. Then, review	45-50 mins

some national and State level initiatives supporting this type of work, and then key considerations from our findings as we move forward with establishing the repository. Next, our goal is to reserve a good chunk of time for Q&A. Please feel free to ask any questions in the chat, and we'll work to respond during the presentation or during the Q&A session. Evelyn and I will be presenting today, and then Nancy and Mark will be chiming in with their expertise as we go.

I wanted to quickly ground ourselves. When we say consent management, we're talking about the systems or processes that let patients decide what health information they're willing to share, with whom, for what purpose, and under what circumstances. Consent is a key enabler for participation in things like patient portals or health information exchanges. It builds the trust and transparency needed for patients to actually engage in this process. Good consent management really allows for flexibility and honors privacy preferences, and ensures that those choices are enforced across the systems.

Consent shows up in multiple ways across health care and social services. We're usually most familiar with consent for treatment, where someone gives permission to receive care. This is well established in medical settings and sometimes in social services as well. There are a lot of special cases like advanced directives and clinical trials where the consent process is more specific. There's also consent for research. This is typically required when someone's personal health information is used in research studies. Today, our focus is on the third area-consent to share. This is when a person agrees to have their personal information shared across different providers or programs which facilitates better and more coordinated care. While not always required by law, consent to share is becoming best practice. It centers individual agency and acknowledges that a person's data sharing should only happen with a person's approval. As we move forward in this presentation, I would like to keep one question in mind, and that is “What role should the Colorado Digital Consent Repository play in managing these three types of consent?”.

Going a bit more in depth, consent to share gives permissions for organizations to

exchange a person's information, to coordinate care. but for that consent to be meaningful, it should be both dynamic (revocable at any time) and granular (allowing people to choose what data is shared, when with whom, and for what purpose). To support this, we need the technical ability to segment data, a system that manages the consent preferences in real time. These types of sharing might cover eligibility and enrollment referrals, demographic info, or disclosures for care coordination.

I'm going to walk through 2 different models, for how consent can be managed and operationalized. The first model is a centralized consent repository. In this approach, an individual's consent is still collected at the local level, but is stored in a central hub that routes and manages data access. Some of the key benefits of this include a faster, more efficient access to data, and the ability to support broader analytics. As far as reporting through centralized infrastructure, the patient has one place to manage their consent and share data rather than having multiple patient portals. That's one of the key benefits. There are also limitations to consider including the requirement of a strong governance system and ongoing maintenance to avoid issues like outdated or duplicate consent records, especially when updates don't flow quickly from local systems.

An alternative to this is the federated model. In this model each organization retains full control over its own data and consent records. There's no single hub where everything is stored. Organizations will send kind of the high level consent, but ultimately it is stored at these individual localities. This allows more control, as data gets shared only when it's needed. However, there is still a need for a governance system as sharing is coordinated under a regional governance framework. Some of the key advantages include real time data accuracy, fewer concerns about central data ownership, and a more resilient architecture. For example, smaller breach targets and less risk of one system goes down. So, for example, if one big system, centralized system. It's a much larger issue rather than just one by system. The trade off, however, is that this model can be complex to manage, especially when it comes to tracking consent across multiple systems without common standards. In particular, interoperability can be limited which may affect how complete or timely the data sharing is.

Finally, I want to review models to obtain consent for sharing participation in this initiative. These include opt-in, opt-out, and granular consent which represent different levels of individual control implementation, complexity, and data accessibility.

Opt-in means that no data is shared unless the individual explicitly gives permission. The patient must actively opt-in to sharing. It promotes high transparency and trust. But it can limit data availability, especially for those who don't or can't take proactive steps.

Opt-out flips the dynamic, where data is shared by default, and individuals have to take action to stop sharing. It supports broader data access and is often easier to scale. This raises real concerns about privacy, awareness, and equity.

Granular consent offers the most tailored and person-centered approach. It allows individuals to decide what specific information is shared, with whom, and for what purpose, but it's also the most complex to implement and sustain. And as a note, in Colorado, the HIE, Contexture, currently uses an opt-out model.

I do want to take some time to review the broader Federal landscape that dictates health consent and data sharing. This slide outlines a handful of key federal laws and regulations that protect individual’s health information. Each one plays a slightly different role, depending on the context, be it healthcare, behavioral health, medicaid or reproductive services. These laws are foundational for understanding how consent functions across the system, and what privacy rules differ, depending on the type of care or data involved. The big thing to note here, though, is that the Federal law sets the minimum standard. It's a floor. States, programs, and organizations can add additional layers of protection. As we look at how to design a consent repository for Colorado, we just need to understand how these policies align with one another. Sometimes they overlap, and the state ones can be more respective.

HIPAA is a foundational regulation in the consent and data privacy landscape; it includes multiple provisions, two of which we'll focus on here-the privacy rule and the

security rule. So the privacy rule is all about who can access protected health information and under what conditions it allows covered entities, like providers and health care plans, to share data without patient authorization for treatment, payment, and operations (commonly referred to as the TPO exception). Outside of that, explicit authorization is required. This includes the use of data for marketing, research, or third party sharing, like sharing with community partners and social services, non covered entities. Another key piece is the minimum necessary standard. Only the data that is truly needed should be disclosed even when sharing is allowed. The security rule complements the privacy rule by requiring specific safeguards to protect the PHI. This includes administrative processes, technical protections, and physical security. For the consent repository, this means implementing strong access controls, encryption, audit logging to track who access what and when. It also means building in role-based permissions, so not everyone sees everything and enabling revocation workflows and the individuals right to access their own data.

Another critical regulation to understand in the context of consent management is 42 CFR Part 2. This federal law governs the confidentiality of substance use disorder treatment, and behavioral and mental health records, and is far more restrictive than HIPAA. Unlike HIPAA, 42 CFR Part 2 requires explicit, written patient consent before sharing identifiable patient related data, even with other providers for treatment purposes. The consent needs to be very specific. It has to name the recipient of the data, describe what the purpose of the disclosure is, define what information will be shared, and acknowledge the patient's right to revoke that consent at any time. Once shared, that patient cannot be redisclosed unless there is separate additional consent. This includes situations where the recipient might otherwise think that they're allowed to share under broader data sharing rules. For the consent repository, we need to make sure we account for the stricter consent requirements and data segmentation to ensure that 42 CFR Part 2 protected information is handled appropriately.

Shifting from the Federal to the State policy landscape, many of the State laws reference the Federal provisions and refer back to them for guidance. This slide organizes key laws by theme so that we can get a sense of just how these policies

work together to define expectations for confidentiality, consent, access, and information security.

For confidentiality, Colorado does have specific confidentiality laws for behavioral health and substance use disorder information. These reinforce or build on 42 CFR Part 2 requiring written and time, limited consent for sharing.

For informed consent, we do see growing emphasis on explicit informed consent. For example, new legislation now requires facilities to disclose non-medical reasons for refusing services, and prohibits intimate exams on unconscious patients without clear consent, data, access, and ownership supporting the HIPAA provisions. Patients in Colorado have the right to inspect and obtain their medical records.

For privacy, data and protection, the Colorado Privacy Act is a more recent law, giving individuals rights over their personal data, including requiring opt-in consent for sensitive data uses.

For security and storage standards, the State has detailed rules around medical record retention and security, especially when a provider closes or transfers a practice. Electronic systems must align with HIPAA, and secure storage and breach protocols are required.

For interoperability and data sharing, there are policies supporting data exchange. For example, there is one in Colorado specifically allowing ambulance records to flow to the HIE, under HIPAA, helping to promote more connected care across settings.

Diving deeper, the Behavioral Health Confidentiality Law. This law brings together multiple statutes and regulations that cover how behavioral health and Substance Use Disorder records are handled in the State. This law builds on federal protections from 42 CFR Part 2 and adds some state specific rules.

- Consent must be time limited
- Any consent to share data must be specific covering who can access it, what is

being shared, and why

- Re-disclosure is prohibited unless the patient gives new and explicit consent

One of the bigger design challenges is the need to support full regulatory adherence. We have to distinguish between the HIPAA, default opt-out model and the 42 CFR Part 2 opt-in model and create separate workflows where needed.

The Colorado Privacy Act expands the conversation beyond healthcare and into the broader realm of consumer data rights. It matters here, though, because health data now comes from a lot more than just doctors offices. It applies to organizations that might not be regulated by HIPAA like wearable device companies, wellness apps or other platforms handling sensitive information. This law is also about putting people in control of their data, how it's used, shared and stored. One of the most significant parts of the law is the requirement for opt-in consent when it comes to sensitive information. These include health, biometric and neural data. It also mandates that people have the right to access, correct, and delete their data, and opt-out of things with targeted advertising which has implications for any 3rd party tools. From a system design standpoint, this means we do need to think about transparency and accountability. The repository may be responsible for things like logging consent activity, limiting data used to its original purpose, and regularly reviewing and deleting data that's no longer needed, especially in sensitive categories. Again, this law is not healthcare specific, but it does create strong expectations for responsible data stewardship.

The last state policy I want to highlight details how we manage, retain, and protect records over time. The rules are detailed in this one. So it's really just a formula that we'd have to follow. Adult records are typically kept for seven to ten years, or minors records need to be held until age 25 or later. That means the Consent Repository may need to track deadlines, alert administrators, and automate some retention workflows. We also need to be precise in how consent is captured, including who will receive the data? For what purpose, what's being shared and how to revoke consent?

Another layer is treatment admission. Patients often provide consent when entering care, but that may need to evolve. So we do need dynamic forms that can be updated as care needs or preferences change. Finally, there's the issue of emergency consent.

Sometimes verbal consent is the only option in a crisis, but this does need to be followed up with in writing within 2 business days, so we do need to make sure that the consent repository can handle any temporary workflows or automated reminders. This policy is very operational, but it does play a big role in ensuring that our consent infrastructure is legally compliant, technically sound, and centered on the patient's long term rights and choices.

Evelyn Gallego:
What are the national and grounding Federal laws and regulations that exist right now around protecting patient and sensitive data? In 2010, there was a criteria for certification of Electronic Health Records (EHRs) and related systems. Within the certification program there is a criteria around supporting security tagging of structured data for exchange, so this is really where we get to a point of how we protect and start looking at tagging our more granular level data exchange.

When we get to 2016-2020, and 2022, we start seeing Federal law and regulation that really starts talking about making data more transparent and open, beginning with the Cures Act of 2016, you have a law that says you must make data available and you have penalties associated with information blocking. So, when we talk about data exchange and having that way to secure data, and we look at these different models, we have law saying, “You still can't block data sharing”. There are challenges around that. Following the Cures Act from a law perspective, you then have the regulations from The Assistant for Secretary of Technology and Policy, known as ONC, who then issues the information blocking rule and conditions of certification for health IT developers. Then CMS, in tangent, has the promoting interoperability rule.

In 2022, TEFCA was released. The Common Agreement was published and establishes a baseline and requirements for secure information exchange. In 2022, the Dobbs vs. Jackson decision around reproductive health was made, which ended up changing a lot of things where the protection of sensitive data became a big discussion.

In 2023 and 2024, we had the US Core for Data Interoperability (USCDI). That is part of ONC's ASTP requirements and also part of the certification where it's saying, "Now, we're going to look at data classes for any level of information exchange between certified technologies". We also now have data classes with standard codes that are required for exchange.

Savanah Mueller:

In this next section. I'll walk through a set of best practices for consent management. They're grounded in both Federal and State law, but they also reflect where we have the chance to go above and beyond. As mentioned before, the legal standards give us a floor. We're working towards building a trusted, person-centered consent infrastructure for Colorado, so until sharing through a centralized consent, repository becomes standard practice, we can lead with these best practices to demonstrate compliance and build public confidence, ensure people feel respected and protected where their data is shared.

Our first best practice, and also legal expectation under both HIPAA and Colorado law, is that consent should be active, informed, and intentional, not buried in general forms, or treated as a checkbox. People should clearly understand what data is being shared, with whom and for what purpose, as I've mentioned many times before, and they should have the opportunity to ask questions and make informed decisions ideally in their preferred language and with materials that are culturally appropriate. This might mean that we need to rethink the existing clinical workflows if consent is being asked for during a busy intake process or tucked into long paperwork. We may need to build in dedicated time clear explanations and staff training to support this. Whether it's done digitally or in person, transparency and clarity should guide the process. When people feel like they actually understand what they're consenting to, then the trust increases, and then so does care.

The second best practice is how we handle consent for sensitive data, things like substance use, disorder records, mental health information, and reproductive health services. Not all of these are protected under 42 CFR Part 2, but mishandling this kind of information can lead to stigma, discrimination, or loss of trust, in addition to violating

42 CFR Part 2 law. We can't treat consent for sensitive data the same as just general health data. It's critical to use distinct and viable consent prompts or forms that explain what the data is, what specific protections apply, and what sharing that information might actually mean. This becomes especially important if the consent repository expands beyond healthcare into spaces more like social services, behavioral health substance use disorder treatment where the data is often more sensitive and governed by a patchwork of regulations. People need to understand what they're consenting to at a deeper level. Systems also need to reflect that with a purposeful design and strong guardrails. It's more than just compliance with 42 CFR Part 2 and the Behavioral Health Confidentiality Law. It's also about building a system that respects the individuals who are using it, especially for communities that maybe have faced greater risks from data misuse.

Our 3rd best practice that we're listing out today is about making sure that people can choose not to share their data, and if they do so, that they can do so easily, confidently, and without fear of consequences. Patients must be clearly informed that opting out is still within their right. Doing so will not affect their care or access to services. It can't be hidden in the fine print or mentioned as an afterthought. If it's electronic, it could be done through pop ups or digital tools in person conversations during intake or a clearly labeled option, and the patient should really feel that their choice is respected. Transparency here is key. Not just that opt-out is available, but that people understand what it means and what data won't be shared. What are the trade-offs? Will they still get the services they need? Opt-out mechanisms are just part of building informed trust, especially if we are moving towards an interoperable consent repository. Trust is really crucial to that long term adoption.

Evelyn Gallego:
The following slides are just to give you a sense of what's happening across the country that can inform the design of the consent repository. I like to show this because I'm a true advocate of not reinventing the wheel, and often in working across different states, states appreciate peer to peer learning.

I'll start with the shift task force. It's a public-private, collaborative. They've been looking at developing use cases and updating existing standards for granular segmentation of sensitive health data. So they have three work streams. All these are open to the public. For shift task force, you do have to sign up to be members, but they are still free. Why is it relevant this work? Because they have existing use cases, and they have started looking at developing terminology. These are coded value sets to represent and exchange this data that can be of consideration for Colorado. They're also updating existing standards, and they're developing privacy policies and defining patient consent preferences. Shift also has sandbox demonstrations. So it could also be a way of being able to see and learn or to participate in their demonstrations. The Sequoia Project is the recognized coordinating entity (RCE) for TEFCA. They stood up a privacy and consent work group. Right now, it is composed of Sequoia members. However, they're in the process of standing up a community of practice that they'll open to the country. In essence, they're a coalition. What's distinct about Sequoia is they're looking at the implementation. So, for those not familiar with Sequoia, they focus a lot on bringing the networks. They're not just HIE focused, but they also include all of the national networks that exist. They are looking at the implementation level because they know how challenging it is to create established consent management infrastructure, so they've been looking at how to do that using technology and computable level. They'll also be standing up pilots. So again, also an opportunity for this work group to listen in and participate. Health Level 7 (HL7) is an international standards development organization. They curate standards for data exchange, mainly focused on clinical. However, they also focus on social determinants of health with the gravity project, public health, research, and AI. They have two groups right now that are open to everyone. You only need to be a paid HL7 member if you want to vote on a standard. Other than that, all are welcome to join. The workgroups they host are focused on developing and enhancing data standards. Carin is also a FHIR accelerator. They've been focused very much on consumer	

mediated or patient level data exchange and advancing the use of FHIR. So again, from a consumer perspective, they bring that together. There is a paid membership for Carin. Carin is interested in identity management, and they've been looking at having consent being driven by at the individual level.

Fast is also an HL7 FHIR accelerator. These are other collaboratives distinct from the work groups, but they all work with one another, and they're about scaling. So they really care about implementation as well as noting why it's relevant. They're currently working on FHIR-based digital consent models and really looking at how to verify consent.

Lastly, we have the stewards of change. Stewards of change has been working on granular consent and consent to share for several years, working also in partnership with HIMSS. They recently published a consent to share service utility conceptual model. They are currently testing this in Chicago. They have a series of tools available. They have a uniform template catalog, consent management, workflo, and taxonomy matrix.

It is clear from all the work to date, and the awareness of the complexity of aligning regulations at the Federal level and at the State level, that there are no uniformity and privacy laws at the Federal and State level. So, of course, it creates challenges for interoperability and compliance.

A few operation and technical challenges are:

- There is no standard workflow for capturing and acting on sensitive data exchange across different systems (EHRs, HIEs, payers, public health)
- Lack of interoperability between state, federal, and private Health IT systems
- Data segmentation solutions are in various stages of adoption that either over-share or block data entirely.

Some key barriers and challenges for computable consent are:

- Legal and policy fragmentation
- Technical challenges in data segmentation and interoperability

- Privacy concerns and patient trust
- Resource constraints and administrative burden

[A poll was presented asking "Given what you just learned, which of the following do you feel is the biggest challenge for creating a centralized digital consent repository?

- **Legal and Policy Complexity**
- **Data Segmentation Challenges**
- **Interoperability and Data Exchange Issues**
- **Provider and Patient Burden**
- **Lack of Standardized Consent Models and Workflows**
- **Other (short answer)]**

[Pause for discussion]

Savanah Mueller:
Next, we will talk about some of the key considerations for designing a consent repository that needs to be compliant, trusted, scalable and equitable. These considerations are directly informed by the challenges and themes that Evelyn surfaced earlier. Some of them are technical, like managing interoperability and granular consent and ensuring HIPAA compliance. Others are more structural, like the complexity of governance or the need for audit trails and consent revocation pathways. And then there's also human centered considerations like addressing the digital divide, ensuring information. Consent is truly informed and making sure that the system doesn't add any unnecessary burden to care teams.

So these 1st 3 areas are just areas that we need to keep in focus when designing a consent repository: governance, revocation and auditability, and equity.

For governance, focusing on a centralized or federated model, we just need a strong multi-agency governance to define roles and responsibilities, make sure legal agreements and policies stay aligned. For revocation and auditability, patients must be

able to change their mind at any time. The system needs to track that. For Equity. If we only offer digital options, we risk leaving some people behind, especially those without internet access or familiarity with technology.

Next, we'll a little bit more into the technical side of implementation. There's granular consent, which I know we touched on quite a bit. Moving beyond the all or nothing models that people can choose to share some information, but not all, does require more sophisticated tools that can tag data by type and purpose. We'll also need to align with national standards. There's also the concern for data fragmentation. Consent workers also live in multiple, disconnected systems which creates a risk of misalignment. And finally, interoperability. Even the best consent management system won't work if they can't talk to the others, so making sure we adopt a standard for formats and protocols.

These considerations focus more on making sure the consensus system is trustworthy, secure, and sustainable. So it's informed consent, not just collecting a signature, and really making sure that patients know what they're agreeing to for security and breach prevention. The repository requires strong encryption, role based access and breach protocols. Workflow and workload is another challenge, especially for smaller providers. If the system feels like an extra burden, it won't be adopted. And then finally, HIPAA compliance. We'll need a privacy officer, or someone in charge of the HIPAA privacy compliance overseeing this.

Before I go, I'd like to ask the following question: What policy, governance, or implementation strategies would you recommend to improve interoperability, legal clarity, and trust in consent exchange across sectors?

Roberta Lopez:
I think one thing that would go a long way for me, and I would assume that it does for others as well, is thinking about the operational pieces. Meaning, are there thoughts about a help desk? What is going to be the interface for providers and for patients, citizens, clients to have the ability to submit an email and get an immediate response

when someone wants to have their data removed. That would go a long way. **Savanah Mueller:** I think that's very valid. For the operational side, we're kind of coming up with these recommendations. One of the next topics that we're going to consider is more of the technical and interoperability feasibility. So I think we'll start to address that as we move into that next topic. **Roberta Lopez:** I would think that the operational piece would include a lot of training and availability for client training as well as provider training and things like that. **Codie Leighton:** Let's say you can't get people to trust the platform. Would you require people to sign up for this consent repository like? **Nancy Lush:** Forcing people to sign up is contrary to building trust. Whatever is proposed or considered ultimately by the State, should consider protecting patient privacy. The whole purpose is to build trust. I think most of the people of this group understand the benefits of good interoperability. And so we try to create systems that will enable interoperability, but also protect the individual patient's needs, and different patients have a variety of different needs. It's a challenge to address them all. But I think that's the goal of what we're trying to achieve here. **Katie Nelson:** There's multiple levels of legal statutes and regulations that apply to consent at the State and Federal level that they went through earlier in the presentation. So even if we could say it's a requirement to sign up for the Colorado Consent Management Repository, we can't change what HIPAA, or 42 CFR Part 2 says, and those are clearly based around informed, patient consent.	
Workgroup Questions and Discussion	20-30 mins

EMI Advisors, Allie McGee, Tiffany Sailler

Codie Leighton:

In trying to understand a granular consent model, how does a person get into the consent repository? And how does a person not get overburdened with multiple consents? Let's say a person needs a lot of help. In this case, an organization would have to send a consent to help them, and then another organization, then another organization. How can we navigate that to make the process as seamless as possible?

Evelyn Gallego:

That's a great question, and that's what we want to solve collectively with you. There is no perfect model to do this right. It continues to be a burden, and a lot of the work from stewards of change is really, how can we have at least a minimal viable product that makes it easier?

Allie McGee:

This is a feasibility study, and this is going to be presented to two different committees in the legislature. So when we're asking folk the question of “What do you think is the biggest challenge for creating a repository?”, I think we need to maybe frame it as “If we were going to put this in front of the folks who have the ability to make the decision of whether this gets created, what do we want them to know, or the challenges?

Jane Wilson:

A couple people have mentioned interoperability challenges. And I wanted to know what you think is the interoperability, regulation, compliance, requirement that we might be working towards when we are thinking about structuring this repository?

Evelyn Gallego:

Interoperability is the seamless exchange of information, electronic information without any burden on the person requesting or sharing the data. So that's really what it is. It ensures that it's transparent, regardless of the data source.

Jane Wilson:

So not necessarily a compliance issue in terms of the interoperability regulations.

Evelyn Gallego:
Correct.

Tiffany Sailler:
I have a couple of things that I wanted to add. There are regulations that do require organizations to exchange data, but those regulations, for the most part, are through CMS like promoting interoperability and MIPS, and not everybody participates in those programs. So if you don't participate in those programs, you may not have any sort of regulatory requirement to data share when it comes to information blocking. So, when reproductive health is talked about, we don't have to block or not share that data. It's not like Part 2. It allows us to not share it and not get in trouble for blocking.

Nancy Lush:
Tiffany, I think I may have misunderstood. To clarify, information blocking also implies that you're not allowed to information block for certain reasons. Correct?

Tiffany Sailler:
There are exclusions or exceptions. There's an exception now that you can hide reproductive data. If a patient comes to seek out abortion care at a facility that performs that care and we were concerned that that patient was going to have some sort of like legal repercussions as a result of doing so, we can make a decision here to not share that data with other providers. And they could not say that we were information blocking, because we would be able to say "There's an exclusion for that, and we've decided to exclude that". It doesn't mean that we have to, though. If we want to share that information because we think it's pertinent to the patient's overall care, that's totally fine. It allows you to do it without getting in trouble for information blocking.

Nancy Lush:
Thank you for that clarification. Also, just to mention that when we're talking about a repository housing consent and then sharing that consent, there's another pattern

where we're not actually sharing the consent, but we compute the consent. That, oftentimes, the consent itself can contain PHI. So, it's not always appropriate to share the consent itself. However, if it's done right and these are actually computable, then there is a vision where you could have a common repository, making it easy for the patient to manage all the consents in one place, but have it be computable in terms of what is shared and not shared. This way, you're not surfacing that “I don't want to have my abortion status shared”, but we're simply not sharing that if that's what the consent dictates.

Tiffany Sailler:
I think one of the complicating things is looking at the technical side when you think about substance use or abortion data. Trying to find all of that information in a medical record and not share gets very complex, very fast, as you can probably imagine. You can make the decision that you’re not going to share this problem, diagnosis, or medication but then there are notes and flow sheets, and many places within an EHR system that people can type notes in. There is no capability for any EHRs to go through and data-mine free text information and pull out certain bits of data so that it's not shared. So even if you make the decision to say, “I don't want to share substance abuse data”, if a person references substance abuse in a note or in a flow sheet, that gets shared.

Alexis Harper:
I just wanted to kind of add on to that. Within the State of Colorado, I've been working to help develop an interoperability platform for jails to exchange information. This has been mostly in the interest of promoting a continuity of care, so as people are transferred between different incarcerative settings, staff are aware of any health and safety concerns about that person coming into their custody. Because we can't really exchange specific information like a specific (HIPAA compliant information or HIPAA protected information), we have a system of alerts that simply just says, there is, or there is not, data to be aware of regarding this person. When it comes to things like notes, we went through that same kind of issue where these free text fields can contain literally anything, so it had to be restricted. We just set up a note within the exchange

between jails. If a data field is coming across that contains what could potentially be confidential information, our data broker essentially writes “There's information here. Contact the reporting agency for that information”. This way, the jail knows what other jail has information, so they can go through that proper channel too to then request the data to manage to exchange that data per HIPAA compliance, for example.

Savanah Mueller:
Thank you, Alexis. I think I remember coming across some of your work in the research and trying to see what was what was currently in existence. We were trying to determine what kind of repositories are in Colorado, so we were looking at some of that.

Alexis Harper:
That's a really important distinction for Colorado Trusted Interoperability Platform (CTIP). It's not a repository. And so we do not store the data. Jails wanted to maintain their local control and data governance over the information that they were willing to exchange with other agencies that have the same goal which is to promote the health and safety of the people in their custody as well as their staff. The State of Colorado agreed that we can facilitate this exchange without storing any of that information, and that allows data governance control to remain with the local agencies.

Nancy Lush:
Thanks, Alexis. That's really helpful information. I appreciate hearing more detail about that, and am really curious to hear whether or not you've introduced the concept of consent for consumers that are incarcerated, and any kind of learnings you've learned in that area as well.

Alexis Harper:
For the most part, there's not a level of consent required for individuals that are incarcerated and receiving treatment. And because we're not exchanging individual level data or storing individual level data and it's just those alerts, we didn't need to go through that process**.** So, we managed to find a capacity for working around that

because we're not exchanging that specific HIPAA protected information. I will say that the platform is CGIS compliant and adheres to CGIS security standards and data exchange standards, because there is PII and other CGIS related information that's being exchanged. But because it's between other agencies of the same level and authority, it just was like a participation agreement that required them to acknowledge the way that this information could be used. Again, it's to the benefit of the people that are experiencing incarceration, so they can know what other agencies to call to have records transferred on a much higher level. There is opportunity, I think, for expansion where consent management would have to come into play. I think that there are other platforms and agencies, even people within this call that have been working with, like the health information exchanges in the State of Colorado, to try to integrate jails to those HIEs, so providers could work in that sort of reentry level capacity, making referrals to community providers as people are transitioning out of incarcerative settings**.** But that's out of my wheelhouse. My sort of arena is specifically within the CTIP for jail information sharing.	
Public Comment and Closing *Allie McGee* No public comment.	5 mins

Follow Up:	**Complete By:**	**Responsible:**