Transcript

HEALTH INFORMATION TECHNOLOGY ADVISORY COMMITTEE (HITAC) ANNUAL REPORT WORKGROUP MEETING

August 5, 2024, 12 – 1:30 PM ET

VIRTUAL

MEMBERS IN ATTENDANCE

Medell Briggs-Malonson, UCLA Health, Co-Chair
Eliel Oliveira, Harvard Medical School & Harvard Pilgrim Health Care Institute, Co-Chair
Shila Blend, North Dakota Health Information Network
Hans Buitendijk, Oracle Health
Steven (Ike) Eichner, Texas Department of State Health Services
Hannah Galvin, Cambridge Health Alliance
Anna McCollister, Individual
Rochelle Prosser, Orchid Healthcare Solutions

MEMBERS NOT IN ATTENDANCE

Sarah DeSilvey, Gravity Project
Jim Jirjis, Centers for Disease Control and Prevention
Kikelomo Oshunkentan, Pegasystems

ONC STAFF

Peter Karras, Acting Designated Federal Officer, ONC
Michelle Murray, Senior Health Policy Analyst, ONC

PRESENTERS

Deven McGraw, Citizen (Discussant)

Call to Order/Roll Call (00:00:00)

Peter Karras
Good morning, everyone, and welcome to the FY24 cycle of the Annual Report Workgroup. I am Peter Karras with Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP), and I would like to thank you for joining us today. I will be serving as the acting Designated Federal Officer for today's call on behalf of Seth Pazinski, and just a reminder that all workgroup meetings are open to the public, and public feedback is welcomed and encouraged. Members of the public can type comments in the Zoom chat feature throughout the meeting or make verbal comments during the public comment period that is scheduled towards the end of today's agenda. I will now begin the meeting with roll call of the workgroup members. When I do call your name, please indicate that you are present. We will first start with our co-chairs. Medell Briggs-Malonson?

Medell Briggs-Malonson
Good afternoon, everyone.

Peter Karras
Good afternoon. Eliel Oliveira?

Eliel Oliveira
Well, good morning for me.

Peter Karras
Good morning, Eliel. Shila Blend?

Shila Blend
Good morning, everyone.

Peter Karras
Good morning. Hans Buitendijk?

Hans Buitendijk
Good day today!

Peter Karras
Good day to you. Sarah DeSilvey? Steve Eichner?

Steven Eichner
Happy Monday.

Peter Karras
Happy Monday. Hannah Galvin?

Hannah Galvin
Good morning.

Peter Karras
Good morning, Hannah. Jim Jirjis? Anna McCollister? Kikelomo Oshunkentan? Rochelle Prosser?

Rochelle Prosser
Good morning, everyone.

Peter Karras
Good morning, Rochelle. Thank you, everyone. Is there anybody who just joined who did not get a chance to indicate their presence or anyone I may have missed? All right, well, thank you, and I will turn it over to our co-chairs for opening remarks.

Opening Remarks (00:02:13)

Medell Briggs-Malonson
Thank you so much, Peter. Good afternoon, good morning, and good day to everyone. It is such a pleasure to be back in our always engaged and exciting Annual Report Workgroup today. I was unable to join our last meeting, but I heard that we were able to make so much progress in our last meeting, so we are going to keep that momentum going and try to get through as much of our crosswalk today as possible. Eliel, I will turn it on over to you for your opening remarks.

Eliel Oliveira

Yes, thank you, Medell, and yes, good day. I will keep it that way to all of you. I am excited to be here today again and continuing the progress. Yes, I agree we made some good progress last time we met, so now, we want to continue on that front, so, thank you, everyone, for joining again and keeping us moving. A special thank you to Deven for joining us as well to discuss privacy and security challenges with her experience. Thank you, Deven.

Update on Workgroup Plans & Discussion of Draft Crosswalk of Topics for the HITAC Annual Report for FY24 (00:03:19)

Medell Briggs-Malonson

We can go right on to the next slide. Just a quick overview of today's agenda is that the next item we are going to focus on is an update on all the workgroup plans, then we are going to go and really spend the vast majority of our time discussing the draft crosswalk of the topics for the HITAC annual report for fiscal year 2024, and as Eliel just mentioned, thank you again. I also want to extend my thanks to Deven for being on the call today in order to lend all of her expertise, especially in the privacy and security aspects. And then we will open it up for public comment near the end of our meeting, and then we will adjourn. Next slide.

So, here is an update on all of our workgroup plans. Next slide. Again, we are making progress. We are almost to the halfway mark, and today, we will continue to review the crosswalk of topics for the annual report. We will also reconvene on August 26th in order to tie up any loose ends of those crosswalks as well. On September 9th, that is when we are really going to move more into developing the draft of the annual report, and then also develop that draft and fine-tuning those details in order to submit it to the full HITAC committee for review. On November 24th, we are going to update the draft with any of the feedback that we receive from the HITAC committee in order to then represent it for final review and approval. Our goal is to have the annual report completely ready and wrapped up in a nice, pretty package before the end of this calendar year in order to submit to our Assistant Secretary Tripathi, as well as Secretary Becerra and the rest of Congress. Next slide.

In terms of the meeting schedule for the full committee, during this upcoming HITAC meeting, which will be next Thursday, we will provide an update on the annual report development. In particular, we are going to discuss the crosswalk, so that is one of the reasons why this meeting today is so incredibly important. Hopefully, we will be able to get through as much of the crosswalk as possible. And then, on September 12th, we will provide another update on the annual report development itself. On October 17th, we will officially review the draft of the annual report, and again, that will be our in-person HITAC committee meeting. On November 7th, we will bring it back to the committee in order for final approval to be transmitted. Next slide.

So, what are our tasks that we are charged with? We are in the middle of drafting the crosswalk topics, identifying the gaps and opportunities, and providing the recommended activities across all of the various different target areas. In addition, we will continue to finalize the review of the draft report that all of our colleagues will help to put together, specifically in September, in order to prepare it to be presented to HITAC in October. After all the additional edits, the HITAC votes to approve the report, and it is transmitted to the Assistant Secretary and National Coordinator in November 2024. And then, of course, ASTP/ONC will then forward that final report to the HHS Secretary and Congress for it to be posted on HealthIT.gov. Next slide.

All right, I think that we can now jump into our business at hand for today. Once again, we had a wonderful discussion last time. We were able to get through several different topics. However, there was one topic that could probably use a little bit more time, so we wanted to go back. Accel team, can we bring up the crosswalk right now? Yes, perfect. We wanted to make sure that everyone did have the time to review this last topic before we jump into the privacy and security topics and others, but had enough time to look at this topic in particular and provide as much input as possible. So, once again, when we look at the topic of provider use of artificial intelligence (AI) in health and healthcare, the gap was as AI capabilities continue to grow, there is a lack of best practices on where the use of AI is clinically appropriate.

The challenge is that problems with data quality relevance and usability can contribute to safety issues and incorrect outputs. The opportunity is assisting and identifying best practices for clinically appropriate uses of AI. And then, some of the proposed recommended HITAC activities from this past meeting were first, request that ASTP identify what AI actually is and is not in healthcare, and especially within their scope, and I think that is very important. In order to help to frame future HITAC AI-related work, explore steps that ASTP, in collaboration with other agencies, can take to establish best practices for appropriate uses of AI in healthcare, and those areas where best practices could include decision support reviewing care summaries for relevant information and assisting patients. And then, exploring the need for AI surveillance programs, similar to existing surveillance programs for drugs to identify issues such as safety or equity concerns. So, there was a large amount of robust activity, but we just wanted to just start up here to see if there are any other thoughts or comments before we move on to the next section. So, let's jump right on in, and Ike, I see your hand.

Steven Eichner
Thank you so much. It occurs to me that one thing we did not address at all is anything about research. We have talked about health and healthcare, but did not touch on research, and not only where the use of AI might be clinically appropriate, but how it might be clinically appropriate. I think those are two different components.

Medell Briggs-Malonson
Those are all very great points, for sure. Any other thoughts as well on this section? And so, really making sure that we are also focused on the research aspects of AI and where some of the safeguards are there, is there anything else that we think in terms of provider use of AI in health and healthcare?

Steven Eichner
This is Steve. Just to elaborate, the same factors come into play for the use of AI in the research side with respect to looking at health equity issues and looking at ensuring we have excellent representation of all potentially impacted individuals when we are using AI regardless of whether we are using it in research, clinical care, etc. That might be another piece of how we link the use of AI and healthcare to coordinate things with social services.

Medell Briggs-Malonson
Absolutely. It is so incredible. We speak all the time during HITAC and in so many other domains about the appropriate representation of all of those who may be impacted by this emerging technology and making sure the voices are there and the perspectives are there, but as you also mentioned, Ike, this should not

just be in a silo for research or clinical care, but also thinking about how we link up our additional social services and how that impacts because all of our technology should be used to advance the greater good of all populations, so, thank you for all of those.

Steven Eichner
Right, and not just for that, but also in coordination, thinking about the kinds of things we have been talking about in other places with health information exchange. One of the goals is trying to reduce duplicative entry of information on the patients. Well, I have the same kind of thoughts about AI from a patient perspective or a provider perspective. How can we implement it once for use across domains so that people do not have to provide the same information in multiple spaces?

Medell Briggs-Malonson
That would be wonderful. Ike, it sounds like what you are doing is coming up with some of the proposed recommended activities, and it goes underneath this area of exploration, just to center it and guide it a bit more. Again, for No. 1., incorporating some of the uses for research in order to advance it over health and healthcare, but also to identify and mitigate any forms of health inequity that may occur. But also something that may go a little bit more into No. 2 as well, the coordination across all of not only our agencies, but also our various different services providers in order to decrease the burden on both providers and patients in terms of the use of these technologies and the information across the space.

Steven Eichner
Right. I guess one way of summing it up, and then I will be quiet, is looking at interoperable AI so that we are looking at the cross-provider space so we are not having all these siloes.

Medell Briggs-Malonson
Correct, yes, absolutely. As we have always said, AI is interwoven into all that we do now, so interoperability is a key area there as well. Thank you for all of those comments and thoughts. Rochelle, I see your hand up next.

Rochelle Prosser
Hi, Medell. Thank you so much. Just taking a step off of Ike and all those before me, I had some time to really drill down and think about this particular one a little bit more. And when we think about children, young adults, and adults with disabilities, are we really actually taking in the components of AI when we bring that into the space? Just as we have our aging population or the aging population with dementia or Alzheimer's, and we want to have them be inclusive in the use of AI, we want to think about our “The Americans with Disabilities Act” (ADA) folks out there where they have learning disabilities, but still can use AI with accommodations and tools. Are we actually bringing them into the fold? That is the first question. Are we thinking about those that are ADA-compliant, and is AI being used in an ADA-compliant way? That is No. 1.

No. 2, for our native Indian or Indian Health nonfederal proponents, when we develop AI, are we thinking of them and the Indian Health Services? Yes, we are talking about public health services, but are we actually being compliant with the laws and tribal laws of their society to ensure full interoperability there? And then, finally, with our lesbian, gay, bisexual, transgender, and queer (LGBTQ) populations, are we being socially

compliant as well, and inclusive in that space? Those are the three things that came to mind as I thought about this particular one, and I am so glad we were able to go back to it today.

Medell Briggs-Malonson
Thank you again for all of those wonderful comments, Rochelle. Just to bring that together, I think these are all very important points because one of the things is that although this says "provider use of AI," it is also important to look at it from the perspectives of the patients themselves in terms of what is acceptable or unacceptable and what is really going to help to engage them in this entire healthcare experience the same. So, whether it is individuals that are living with physical or cognitive disabilities, but also thinking about some of the specific needs as well in terms of the accessibility and accommodations of these tools so that providers are being able to be inclusive of this technology with all these patients, but definitely, yes, with our LGBTQ+ community, are there things that would be more acceptable? And I would say that across all of our marginalized populations.

I think with the Indian Health Services, we do try to bring in as much of the input as well, of course, from our tribal agency, but really being very thoughtful of saying we should make sure we are including this important group of experts and agencies into the space too to see what is possible. Thank you for that. These are all great proposed recommended HITAC activities so that we can be very explicit with this.

Anna, I see your hand, and I am going to say one quick thing, too. There is one thing I want to add here. We have spoken about what is clinically appropriate and what is appropriate for research and interoperability, and also from the patient lens.

There is one thing I think is something that I notice is missing here, and I know that ASTP does not normally frame it this way, but as a physician, I actually frame it this way. And that is some of the administrative clinical uses of AI itself because we know that there is a lot of new AI technology that is actually helping or trying to help us be more efficient. However, there are also some privacy questions and concerns, which is why I am happy that Deven is here as we talk about more of these areas, but as this blossoming ecosystem is expanding, I think it is very important to think about some of the appropriate and important administrative uses of AI in healthcare by providers because we have to really be thoughtful and make sure that we are still engaging the trust of our patient populations and our communities while also ensuring that we are not over-relying on some of this admin AI as well. That is one thing I want to add to the conversation to be captured also. Anna, I see your hand, and then we will go to Eliel.

Anna McCollister
Thanks, Medell. First of all, my apologies, because in the past, I have had conflicts that I could not change over the past couple of meetings, so I am kind of behind the curve in terms of being up to speed on what the prior discussions have been. I am trying to understand a couple of things. First, exactly what is it that we are recommending here? What Rochelle just walked through is super important, but it seems to me that this is really focused on provider use of AI in health and healthcare. So, maybe if you are thinking about training data or that kind of thing? Anyway, I just want to make sure I understand the thing correctly.

It looks as if we are just focused here on telling ONC/ASTP that they need to put together some workgroups or task forces to really explore this. Am I reading that correctly? So, for instance, the big things that I am concerned about within the context of provider use of AI are things like if they are using AI that has been

trained with clunky, not-so-well-curated and normalized clinical data. When I look at the data download that I have from my medical record, it is kind of terrifying to think that that is going to be fed into an AI algorithm and used for clinical decisions.

So, there is that. And the other thing is something that Zack Coney posted this morning on LinkedIn. How if you took the American Heart Association's risk stratification algorithm and applied it to most people about use of statins and antihypertensives, we would see an increase in cardiovascular events and MI. So that is the kind of AI that I am really concerned about. Because you have the American Heart Association, which everybody respects and says, "Well, if these guys say that it is good, then it has to be good," and if that were incorporated whole-cloth into an Epic or Cerner electronic health record (EHR) or a major hospital system's EHR, then the consequences could be really bad, both in the long term as well as in the short term, in terms of getting access for patients. To me, that is the kind of stuff that I would like ONC to really explore. How do we keep the bad things from happening while not creating barriers for the good things to happen? We need to have AI in healthcare; it just needs to be done appropriately, and with caution.

Medell Briggs-Malonson
Absolutely. Thank you, Anna. Yes, this topic is specifically with provider use of AI. However, like Rochelle was saying, there is consideration of some of the patient aspects of this. But your point is well taken, and that is exactly what this is all about. We know that a lot of our AI data models are not representative, they are not high quality, there are several different gaps, they were taken from multiple different sources, and therefore, if you are going to build clinical algorithms or predictive analytics on them, you have to be incredibly cautious because they can actually output erroneous information that then clinically will be acted upon, and as you can see, that is where the challenges come into play here. But I think what you are saying is very, very important, and I am thinking maybe we can clean this up.

From all the comments, we may be able to clean this up on the back end and bring it back up to our Annual Report Workgroup because we do have to make sure all of our proposed recommended activities directly address the challenges that we have identified, and we know that while there is a lot of great good in this, we also want to be very cautious in how we proceed, making sure that ASTP are making those recommendations of how they can assure the quality, the relevance, the usability, and the safety of all of these various different AI algorithms, again, within their scope, because that is always the main thing, or help to be an influence on the other agencies as well. So, Anna, I agree exactly with what you are saying. While our recommendations for this are so incredibly broad and have so many implications, we do also have to think about how we think about it from a provider lens, but also taking in that patient voice and perspective, too, so, thank you.

Anna McCollister
Well, obviously, I care a lot about that patient voice and perspective. Rochelle, that was not meant as a criticism in any way. I am just trying to get my head around exactly what we are trying to focus on. But regardless of whether you have a rare disease, come from an ethnic or tribal minority, or whatever, if you need heart medication, you want your heart medication. The American Heart Association (AHA) algorithm would not necessarily be a good thing regardless of skin color, ethnic whatever. So, that, too, is a big patient concern.

Medell Briggs-Malonson

One hundred percent, yes. Thank you, Anna. We will go to Eliel, and then turn it on over to him to jump into the other section.

Eliel Oliveira
I agree, Anna. What we are trying to achieve here is exactly in line with what you are saying. AI is visibly taking the whole world by surprise, if you will, though not really, as I have been dealing with it for close to 30 years now, but now the genie is out of the lamp, so everybody is looking at it. Every day, we see so much happening in healthcare specifically with AI. Some of it is very useful, like Medell was saying, in terms of administrative tools, but we are basically trying to highlight the areas of concern here without impeding the evolution to deliver better care to all. So, if I were thinking about this, two things would come to mind. First, we have that column of the proposed tier. Digital money is Tier No. 1, right away, because I think this is so important, and we see the movement coming and not stopping.

The second thing I was going to say on that proposed recommendation is about the announcement you all saw last week by ASTP/ONC on Chief Technology Officer, Chief Data Officer, and Chief AI Officer. To me, they all fall under this umbrella and somehow come to strategize with us and with others what they should look like, and what I mean by that is that the points that Steve made were terrific, and so were yours and Rochelle's. They need so much to be addressed, and we just do not have a framework, and I think those individuals that HHS are bringing to the table could be very helpful with this group and HITAC to just look at what we did last time we had an in-person meeting, the hearing that we had, and these discussions here, but really start to open this up to develop exactly what framework we are talking about here. How do we qualify AI for administrative purposes, clinical care, decision support, or some other purposes, like public health, as Steve was saying? Once we have these categories, which I am just making up as I go here, how do we then formalize the process in a way that becomes usable?

I do not know what that definition is either, but I think that is where a task force and these new hires that ONC/ASTP is bringing to the table could help us organize. In our in-person hearing, Peter Embi presented a framework on how data, AI, and research could work. We have done the same thing in our projects here at Harvard, but I think it is still open out there. There has not been a clear definition, so maybe the proposed recommendation is for us to bring in these new leaders and HITAC to develop a task force to work on this, and I think it is going to take a while for us to formalize how AI is going to work in healthcare fully. Sorry, that was quite a bit. Thank you.

Medell Briggs-Malonson
Okay, excellent discussion. Any other items? Let's think about this, but we are going to take all of the feedback, and when we come back to our next meeting, we will make sure that this crosswalk is a little bit more defined and a little bit clearer in terms of all of the different comments that were mentioned, so thank you all for that. Let's keep on moving through the crosswalk. We get to go to privacy and security. Eliel, I will turn it on over to you to walk us through this target area.

Eliel Oliveira
Thanks, Medell, and again, thanks, Deven, for joining us. We are excited to hear your thoughts as well. There is quite a bit here on privacy and security, and as you all know, this is an ongoing target area for the annual report. So, we started with the first one here, which is privacy of sensitive health data in general. The gap that we see is that there is still a lack of consensus on the definition of sensitive health data and

how to implement data segmentation. The challenge is the health IT infrastructure has a limited ability to support identifying and segmenting coded and discrete data that is considered sensitive, and the ability to manage applicable privacy and security rules that apply to sensitive health data, including behavioral health data, presents a challenge to exchange for providers.

The opportunity we see is to gain a consensus on the definition of sensitive data and examine opportunities to increase the availability of certified health IT modules that can manage applicable privacy and security rules to enable data exchange, including for behavioral health. And then, we had some proposed activities here on that front right away, which would be to evaluate the current models and suggest steps toward a terminology value set for sensitive health data elements that could be widely adopted. And then we added that we could explore additional certification needs for health IT systems to support the privacy and security of sensitive data with acute and ambulatory providers that have already adopted certified IT modules, including the needs of behavioral health providers and others that still do not use certified EHR systems. So, with that, that is how we are thinking at a high level that we need to improve the exchange of information by clearly defining what sensitive health data is and being able to collaborate across different types of providers that may or may not use certified systems. So, with that, I will stop there and see if there are any thoughts. Hans, I see your hand up.

Hans Buitendijk
Yes, thank you. I have a couple of thoughts, and not a clear recommendation or suggestion yet, but there are a couple things. And I am reading both the sensitive data and the general and consent together, so some of the comments will blend. I think some of the terminology that we use, like “data segmentation,” gives the impression that we are isolating data and storing it separately. I think we very much want to make sure that in the terminology that we use, it is about recognizing categorizing data that we understand what we can do with it, not necessarily that it means it is physically isolated. But that as a result, we are not sharing it or are sharing it with whomever sits on the other side that can get that. So, I think we just want to be careful with the term “segmentation” as not being a physical intent.

Within “sensitive data,” I think it is increasingly helpful to distinguish between the actual data that we can recognize directly that is sensitive, such as actual condition codes, procedure codes, medications, and otherwise, and categories of data where a document can contain sensitive data, but there is a sensitive flag to indicate that there is something in there, which is not the same. So, we need to make sure we interpret “sensitive data” broadly, not just on individual data, but as part of data sets and documents that it contains there.

The last comment is around the focus on certifying health IT modules, where I think we need to be very broad as well, because when we are looking at it, there are already elements of what… If you will, I am not just going to specifically use an EHR as a data source, but the actual privacy rules that drive what data can be shared may be kept completely in a different area that is centrally accessible, where all the privacy rules across a jurisdiction may be available, at whatever level we do that. So, it is not only that we need to look at the typical IT modules that we think about, the EHRs, the data sources, and what they need to do, but what are these other modules that enable privacy rules to be computably documented, shareable, and accessible, and do the same on the consent side for the patient, that their rules are available, which may not be in the EHR itself, it might be somewhere else because that is where the central store for that patient is.

So, from a terminology perspective, I am going to put it a little more extremely than is intended, but we do not want to give the impression that everything must be part of an EHR. It is actually all those modules together that are going to make it happen, and therefore there also needs to be the infrastructure where, as an EHR, I know where to get access to the privacy rules and to the patient consent. It could be in mine, but it might be in somebody else's. It might be kept with the state or whomever. So, how do we do that in a much more federated model than assuming that everything is EHR-centric? Some of the terminology that we have right now, based on the history behind how we came about certification and everything else, implies for many people an EHR-specific focus. I think we have to step away from that. It is not just EHR that is going to solve it.

Eliel Oliveira

These are excellent thoughts, Hans, and as you are speaking, I am just taking my mind to my health information exchange (HIE) role, which we deal with in Health Insurance Portability and Accountability Act (HIPAA) data for Treatment, Payment, and Operations (TPO) constantly, which basically means we have a clear definition of what are the 18 data elements that are considered Protected Health Information (PHI), when we can allow someone to access them or not and for what reasons, and whether the tools that were built for exchange even allow that. I will give you an example. So, when someone is in an Emergency Medical Services (EMS) truck, EMS accesses the health information exchange to get records about that patient. It is the first time EMS is visiting them or seeing them, so it is not technically their patient, but it is right now, so they break the glass, and there is a feature in the technology that allows that to happen so that, in an emergency, someone can look at the records if it is not their patient.

It is very clearly laid out, and the technology allows that to happen for those use cases, but we do not have that same pathway. At least I have been out enough in the HIE space that many of us just decide not to store and manage 42 Code of Federal Regulations (CFR) Part 2 data because we do not know the variability of what can be done, what situations, what providers, and in which states, so I think what you are describing falls in line with how more specifically we define this, being careful with the segmentation aspect. We are not putting things in different places. That is how HIEs manage data. Everything is in one place, but we do know what can be done and not done for TPO but not for behavioral health and a few other aspects. Thank you for those thoughts. Those are right in line with what we are trying to do here. Deven, I see you have your hand up as well.

Deven McGraw

I do, thank you. I have a couple of thoughts. I largely agree with Hans's comments, although there is one class of data for which the protections do assume that that data is kept separately, and that is psychotherapy notes. The additional protections in the HIPAA privacy rule for psychotherapy notes only apply if that data is separate from the other data. I don't know if there are any other laws that affirmatively require separateness, but as a note, there are some circumstances where it has to be kept separate, or else the additional protections actually do not apply, and that is psychotherapy notes in HIPAA.

The second thing I will say is that I do not know that there is a value proposition to getting consensus on sensitive data because we do have some laws that require certain types and categories of data to be usually subject to additional consent, which then begs the question about why we need two separate categories here, one on consent and one on protections for sensitive data, since, most of the time, except for in the

example I just provided around the separateness requirement, it is really about additional consent requirements that might attach.

But you have the right of people to ask for restrictions. It does not necessarily have to be honored in the case of HIPAA, but that allows the individual to determine what constitutes a sensitive point of data for them. In the context of domestic violence, for example, there are classes of data that might be very sensitive that we would otherwise not consider generally to be sensitive, just looking at them on their face, and it really is personally dependent. So, I personally do not see the value proposition around trying to define what constitutes sensitive data versus assuming that there will be data that needs additional protection, some of it due to law, some of it due to patient sensitivity, and then what happens from there.

The other thing I will say about Part 2 is that that might be worth further exploration because the law has changed in terms of your ability to do TPO with behavioral health data that is subject to Part 2. Once you get an initial consent, that can be much broader than it used to be. It does not have to be provider-specific anymore. So, there are lots of opportunities there to think both from a policy and technology perspective about how to enable the sharing of data because those rules were intentionally changed to try to treat it more like TPO, frankly. I will stop there. Thank you.

Eliel Oliveira
Thank you, Deven. Go ahead, Medell.

Medell Briggs-Malonson
Eliel, there may be some questions for Deven, so I just wanted to open that up. Deven, thank you. That was incredibly helpful. Are there any questions for Deven? Deven is here as our subject matter expert in this space.

Deven McGraw
And Hannah is a subject matter expert too, on many different topics.

Medell Briggs-Malonson
I just wanted to pause to see if there are any questions. I did have a question for Deven, but are there any other questions specifically for Deven on what she just mentioned?

Rochelle Prosser
Actually, I had one. Thank you, Deven, for clarifying that. My thought on the proposal here was to ensure that we can have a proper follow-up in understanding that, in the behavioral health space, you recommend and send for treatment, but there are so many TPO protections there that you mention that it becomes almost impossible for the treating physicians or the working-in-collaboration physicians to ensure that the patient went to treatment, or even verified that they did show up, or even made the appointment. It is just that basic level of communication.

My understanding of what was being proposed is just that we can trust but verify, not necessarily needing to delve into the protectiveness of whether they are in psychotherapy or what was actually being done. Sometimes, on the claims data, you can see that they are, but you cannot even verify with that provider if they actually showed up in their office. And so, this is where my thinking was in looking at the interoperability

and providing a little bit of a lifting of the veil, not necessarily on the protected health data, but just the basic communications. I do not know if anyone else is thinking of it in these terms, and I would love clarification on that.

Medell Briggs-Malonson
Deven, before you answer, I will jump in and add my question to that, too, because it is a little bit like Rochelle's. For instance, in my role, I oversee gender health, and especially when it comes to gender-affirming treatment and reproductive rights, we know that there are a lot of efforts going on across the country with variation in terms of what is acceptable or not in certain states. So, in my mind, the privacy of sensitive health data was for some of these other areas, including behavioral health, in order to allow protection for patients as well as for the providers, so I would love to get some of your thoughts on that.

Eliel Oliveira
Can I add another twist here, Deven? In my case, we are dealing with individuals that are part of the incarceration system and are being treated in clinics in the incarceration system, and we are trying to help by integrating data, but like Rochelle was saying, we do not necessarily need the details about the clinical aspects themselves, but we do not know what to do with the fact that someone is coming out of the incarceration system. Do we tell the providers or not? What are the local, state, regional, and federal limitations to doing that? It becomes very tricky. So, we end up not doing anything and not helping as much.

Deven McGraw
Yes, that happens a lot. There is a sense that this data is too laden down in terms of laws and sensitivity, so people just will not deal with it. That has definitely historically happened. I will say a couple of things in response to some of these comments. First off, the protections for psychotherapy notes are not protections for the fact that someone is in psychotherapy, or even whether they attended the appointment or not. It is the notes from the session. That is it, the notes from the session. So, someone taking notes about what was said in the session is the only thing that that applies to. It does not apply to the drugs or the fact that someone was in psychotherapy.

Similarly, around some of the Part 2 provisions, again, I think it is worth a more complete exploration of the ways that those laws have changed because I think it really has not sunk in. People are still operating under the old framework and not even reconsidering what the possibilities are. There is still a consent required, but it can be obtained at the initial start of treatment, it can apply broadly to subsequent care, so it is much more…not malleable, that is probably not exactly the right word, but it is much more workable than the part used to be.

Often, particular laws associated with prison medical systems and what kind of information can be disclosed might require a much deeper dive into continuity of care for people in the justice system when they are released and obtaining care outside of that system, or even the back-and-forth nature of some of that with respect to certain populations where they might cycle in and out, mostly of jail, not prison, but there are some complications associated with that that do not exist for populations that are not in the justice-involved piece of it. Maybe it is worth some further exploration, but I think there is definitely room for much greater education about what is possible because I think some of what holds us back is overly conservative interpretation, and not a full appreciation of what kinds of behaviors are going to be permissible under the new provisions on Part 2. I do not know if I covered all of it. There was a lot. I might have missed something.

Eliel Oliveira
There is a lot there, Deven, but I think you hit the nail on the head. Yes, there are overconservative ways to manage because folks are just not clear, and that is part of it as well.

Deven McGraw
Yes. When I was working for the Office for Civil Rights, I would often get "HIPAA will not let us do X." That is not true. HIPAA totally lets you do that. I do not know who told you it did not. As a regulator, I could not tell people, "You are claiming HIPAA says you cannot share something when you can." Frankly, that is what the information-blocking rules were supposed to be about. Do not hide behind HIPAA if it is not true, but at the same time, it is mostly an issue of misinterpretation over many, many years. I will stop.

Rochelle Prosser
Do you mind just addressing our other cochair with the maternal health and regional vulnerable population protections?

Deven McGraw
Yes. So, this is another one where I feel like it is very similar to the domestic violence example that I gave earlier, which is it is the kind of care that might frankly not be subject to a particular law that protects it. But it may, in fact, be quite sensitive in the eyes of the patient who is receiving that care or the medical provider who is providing it in terms of a desire to create some protections around how it gets shared going forward. And it is the reason why I think we need to be careful about saying that we have to define what constitutes sensitive data because in many contexts, perceived gender or gender is not considered to be sensitive. But in some contexts, in fact, it is sensitive if the gender is not the gender from birth any longer and has been changed in some way, or not. You all know the circumstances far better than I do, but I just think it is another example.

And then, of course, with reproductive health, many states have passed protections in the law. And after the *Dobbs* decision, there have been even more protections in certain states around the sharing of that data. And I would bucket the repro laws in the bucket that now we have law, in addition to maybe where you do not have law. And there are sensitivities expressed by the patient or, in the case of reproductive health, a medical provider who may, in fact, be in jeopardy when the data flows to places where it could be used against that medical provider. It is just a danger associated with deciding where you are going to define and get consensus on what constitutes sensitivity because it is going to be contextual in many cases and legal in some, and I think we need to be careful about that.

Eliel Oliveira
Thank you so much, Deven. I think all those thoughts and questions highlight really well the importance of education. I do not feel comfortable in many of the situations that we are talking about here. I am hearing that others feel the same way. I am even thinking about how to go about this. It is such a big challenge to strategically address these all the time. One thing I think I heard from you before, Deven, was that we have been talking about privacy and security for a while, and it goes back around. How do we then at least put a plan forward that allows us to make incremental adjustments or educational aspects to solve some of these? Because otherwise, we come back to the same challenges again, and nobody knows what to do, and we end up doing nothing overall.

Hannah Galvin

Eliel, that is a great segue to some of my comments. I do want to say I agree 100% with Deven, and she and I have been working closely in this space for a number of years. And to that point, we do have some history of stakeholders trying to look at data elements one by one and saying, "Is this sensitive or not?", and it has not been effective. This is not without trial and without precedent. But we have been looking at the laws and looking at state-by-state as well as federal laws. And I put a link in the chat that came out recently where we went through and tried to analyze the reproductive health laws state by state post-*Dobbs.* And as Deven said, adolescence is big in looking at it from a legal aspect.

But also, as Deven astutely mentioned, there is a lot of data that is sensitive just because it is sensitive to me because of my previous experience and stigma that may not be protected by law. So, some of the functionality that we are building allows for more algorithmic definition based on the law, as well as patient-specific requested redactions under HIPAA. And I think what you are getting to is really what I wanted to get to. What are the next steps here? We do have people working on terminology value sets right now. The National Association of Community Health Centers has done some great work and is doing some great work with Steven Lane and Shift moving forward to try to come up with terminology value sets and are early in that process, but there is some work being done on that. There is work being done on standards and maturing the standards around this.

And so, what are our next steps to move us forward as opposed to continuing to spin on it where, every time we bring it up, we are like, "Yes, this is really hard, sensitive data is really hard"? My recommendation there is really working through Trusted Exchange Framework and Common Agreement (TEFCA) and working through a standard operating procedure (SOP) in TEFCA as we think about certification. I would advocate that there be a TEFCA SOP requiring granular data privacy protections and consent and bringing these two together, as I think Eliel or someone else recommended, that these two really go together. Deven is the cochair of the Sequoia Privacy Consent Workgroup that several of us are also part of. I see that as the pathway to getting this implemented. Deven, I do not know if you want to speak to this further, but Shift is doing a lot of work on the standards development on the terminology pieces. But in order to get this moving forward from a policy perspective, I would work through the TEFCA framework.

Steven Eichner

Before Deven responds, I want to add in one or two really fast points. No. 1, looking at confidentiality and patient consent as well, where does that actually fit in as sharing under PTO? So, if we are looking at making a recommendation under sharing data under TEFCA, there also needs to be a tie-in as to what is permissible sharing under PTO because operations could be a large opportunity for sharing data. How does that actually mesh in with patient preferences and patient consent in this new space? We need a framework where patients really can control what information is being shared in different environments, and again, looking at the accountability on the back side about where this data is actually being shared right now, there is nothing in TEFCA that has any audit facility at all for reviewing what information has actually been shared. If disclosures that are PTO do not have to be recorded, there is really no method for a patient to audit what was released under PTO.

Medell Briggs-Malonson

Ike, I am going to try to get us back on track. I know there is a lot of robust conversation, but I want to make sure everyone gets a chance to speak, and I know Hans has patiently had his hand up. Ike, we will come back, and Shila, I saw that you also had a comment. We are going to run through this because we still have a lot of things to talk about. So, Hans, please let us know some of your thoughts, and then we will continue to go back through if there are any additional thoughts.

Hans Buitendijk
Thank you, Medell. I have two comments, one in reaction to Deven and this last conversation of if we can define sensitive data, and the other one on TEFCA or the scope of what we need to address. Maybe I will start with the last one first because it is a little bit easier, in a way. We need to make sure that this works, no matter whether there is a TEFCA/HIE state or whatever in between. There is a lot of communication going on, and there will be for a long time to come, that is not necessarily going through a network. It might facilitate some things, but it will be a long time before that is all in place. I think we always have to look at it. It can work regardless of whether it is TEFCA, an HIE, or a state. It just needs to work dynamically in some fashion. That does not mean that there could not be helpful steppingstones to getting some wider adoption. In that sense, I agree, but the solution cannot be dependent on it.

The other part is about sensitive data. I would agree and understand that we cannot define all the sensitive data, and perhaps we need to clarify that we need to have computable rules, which, in turn, need to understand exactly what data is subject to that rule. Unless we aim for that, which is not going to be easy, we are bound to require that every transaction is going to be reviewed by a human. That is not what we would like to have here to facilitate expedient, proper exchange of the data that the right people can get, and the people who are not authorized to get it are not going to get it based on the automated exchange of data that is happening, such as automatic queries, preparation for a next visit, and what I am going to share.

So, I would be cautious in saying that we do not need to know the sensitive data. In a way, we do, but it might not be that we have to define a set that is fixed or is changeable in that fashion, but the rule, whether it is a California rule, a Maryland rule, or my rule as a patient with a directive, needs to tie to the actual characteristics of the data so that either the data itself, like a certain condition, demographic, or lab result I do not want to share. And if that is contained in a document, I have agreement on what the flags are, but as that data is moving around, we do not want to have to chase that data down and say, “Oh, Hans changed his mind. Today, he was willing to share, but tomorrow, he will not be.”

If the data is unique to the data source, but not to us collectively, I am not going to be able to chase down where it has gone. So I think there is an element of sensitive data that has to be defined so I can compute it. Because unless we are willing to accept that people are always going to have to evaluate every query that comes in, whether it is Fast Healthcare Interoperability Resources (FHIR)-based, Clinical Document Architecture (CDA)-based, Version 2-based, proprietary, or whatever, and we need to share it, they have to evaluate it. I do not think that is what we were trying to achieve with interoperability. We want to make sure the right person has access and the wrong person does not have access. How do we do that in a supportive fashion?

Medell Briggs-Malonson
Excellent points, Hans. Thank you so much for that. I think we are now starting to coalesce on some of the different thoughts or recommendations that we have. So it may not be the specific subsets, but the

definitions of what sensitive health data is, and then allowance of those specific flaggings, but it has to be consistent across the various different forms of technology, so thank you for that, Hans. Any other thoughts or comments on this topic? Obviously, there is a lot for us to think of. What I ask of the workgroup is to continue to think about this. Our teams at ASTP will actually try to put all of our comments together, and we will try to revise some of this. But I ask for you all to continue to think and provide your comments, even offline, so that we can get this as tight and as impactful as we want it to be. Any other thoughts or comments here? Shila, I know I saw your hand. I want to make sure we do not miss you.

Shila Blend
Oh, I was going to reiterate and punch it in the comments. What I was thinking is that as we look at this technology, especially with 42 CFR, I know one of the challenges is that HIEs can assist a lot, but there needs to be the consent management, the ability to do that consent, and I know a challenge right now for many is if a patient withdraws that consent, how do they handle it? So, whatever we recommend, we need to ensure that the capabilities are there, that it helps enhance the sharing with the privacy laws in place instead of restricting them, and from the comments that others have posted, I feel that that point has been brought across.

Medell Briggs-Malonson
Wonderful. Well, your points are also very well taken, so thank you so much for sharing with us. All right, that was a wonderful, robust conversation. There is so much for us to think of. As we continue on, before our next meeting, if you have other thoughts, let's send them in so that we can coalesce them together, and when we review the crosswalk next meeting, we can have some of this a little bit more defined about what our recommendations are. Excellent.

All right, Accel, let's keep on going. Let's see how much we can still review within this target area. There we go.

So, the next topic here is lack of disclosure accountability. Patients have limited transparency into how their health data is shared. The challenge is with the growth in exchange, it is important to balance increased transparency to consumers with the burden on organizations that hold data to provide an accounting of disclosures. The opportunity we have is to define a long-term roadmap to implement accounting of disclosures. And at least some of the initial proposed recommended HITAC activities include proposing a national foundation for implementing accounting of disclosures and recommending a simplified model of accounting of disclosures that is concise, involves patients in its development, and considers readers' health literacy level. All right, we will pause there. Any initial thoughts or additions to this area? Yes, Deven?

Deven McGraw
So, this is one where I think I might be teed up to give you all a bit more background about how this issue came to a predecessor committee, the one that was established under the Health Information Technology for Economic and Clinical Health Act (HITECH), the Federal Health IT Policy Committee, which did a hearing on this issue, collected testimony on this issue, and came up with a set of recommendations. I am not sure that the capabilities of EHRs have gotten any better in terms of being able to isolate disclosures that come out of a provider organization that go outside to somebody else versus when somebody just accesses a record internally. And there is a whole history of Office for Civil Rights (OCR) attempting to

initially address accounting of disclosures, which already was expanded in HITECH to include TPO disclosures for electronic health record data.

They originally said what patients should get is an access report, "Any time someone hit the record, whether it is a disclosure or internal access, since there is no way to tell the difference, we will give patients all of it." And we got a lot of concerns expressed in the healthcare provider community about that, so, consequently, a different set of recommendations came out of the Health IT Policy Committee, which I do not have in front of me. I was intending to be prepared next time to talk about it. Having said all of that, as we move into networked environments, there might be far greater opportunities to create records of when someone's data has moved through these systems.

The answer to that may be that it is not any easier than it was to account for disclosures out of an EMR. But that may be worth exploring because then you have an opportunity to actually get at disclosures that left the facility in some more consistent way versus the report of access that frankly could reach from the floor to the ceiling if it were printed out on paper, depending on the complexity of a person's condition for any particular episode of care. At any rate, I will stop there, but I was asked to provide you with a little bit more background on this at a meeting that is coming up in a couple of weeks.

Medell Briggs-Malonson
Oh, great, and already, the context that you provided is very helpful, especially that recommendation of all disclosures internally, but really looking at the disclosures externally, if I understand it correctly, because those, of course, would be some of the most high-risk forms of disclosure that we should take a look at. That is one of them. We look forward to even more context in the upcoming meeting, so, thank you for that. Anna, I see your hand as well.

Anna McCollister
Deven knows how much these issues mean to me, and she and I have had many discussions about these issues, and particularly both this one and the following one are ones that drive me crazy. The only comment that I would make to Deven is that it has been a while since that report came out, and if it has not advanced, it should have advanced. So, part of what we are doing… If the technical capabilities have not advanced, they should have advanced. I do not know; I have no ability to assess where we are, and I was not a member of the HIT Policy Committee and was not involved in the process, but I remember when it was going on.

So, the point of what we are doing here is recommending to ONC, and I guess also to Congress, what kinds of things need to be prioritized. And unless we say that this has to be a priority, I feel like it is never going to happen. I hear you in terms of the stack of paper from here to the ceiling in terms of the number of incidental data access points within a hospital. There has to be a way to summarize those or categorize administrative access for billing, processing, or physician access. There has to be a way to summarize those accesses up into a category that could be shared. So, again, obviously, you have spent more time focusing on this than I have, but I feel like we have to demand that this is a priority; otherwise, it is never going to happen.

Medell Briggs-Malonson

Those are all good points, Anna. Deven, do you, or even Hannah, who is also in this space, know if there has been any additional movement with trying to see where our current state is in terms of capturing and monitoring account disclosures?

Deven McGraw
I do not believe so. There has never been any rulemaking from OCR to implement the HITECH provision after they initially proposed the access report, and they never finalized it. When I was at OCR and we got a new director in the change of administration, he was very frustrated. "Why has this not been done yet? It has been years!" They still did not do it during his term, either. At the time, there were a series of technical challenges associated with it that did not get addressed. There were recommendations to pilot technologies to do it that were not ever done. It remains one of those unimplemented provisions for a bunch of reasons, but yes, it is always helpful to explore what happened before, in what we are in a different space now, and how we can move this forward.

Anna McCollister
Deven, remind me. I feel like you have told me before that this is actually written into statute somewhere.

Deven McGraw
Oh, it is. It is in the HITECH law. TPO exception does not apply when you are disclosing information out of an electronic medical record. But if OCR, who would be the ones to enforce it, does not do regulations to implement it, then it is not worth the paper it is written on.

Anna McCollister
And that is 20 years old, I think.

Deven McGraw
That was 2009.

Anna McCollister
So, unless we, as a workgroup, say that this is a priority, that it has been written into statute for 20 years, nobody will think about it.

Deven McGraw
Yes, but my preference would be to have a way to implement it that would not continue to throw bricks at an immovable wall.

Medell Briggs-Malonson
So, this is obviously a very clear opportunity for improvement and opportunity to explore, and also possibly a recommendation from our workgroup and HITAC to explore how to do this and the appropriate way to remove those barriers, so those are all excellent insights. Hannah, I see your hand as well.

Hannah Galvin
What I will add here actually pertains to both this and the next topic as well. With all of the conversations that I have had around this, as Deven mentioned, there are technical limitations to this in all the ways that the data are shared across the ecosystem. There are also operational and educational concerns that

typically come up in these conversations, which goes to the next topic as well. The ecosystem and the ways that data are shared are so complicated. And I think many patients have a sense that their primary care doctor is sharing data with their specialists, maybe their pharmacist and radiologist, and that is it, but most individuals do not have a great understanding of value-based care and how reimbursement really works. Or the fact that when you send a prescription to the pharmacy, it goes through a pharmacy benefit manager, and somebody there may take a look at the data in order to determine benefits eligibility.

And so, if you open this up and say, "Okay, for anybody who has looked at the patient's data, a report will be generated," a lot of underlying education is needed first to understand where all the data is going. And it is the same thing with deidentified data, in order not to cause mass confusion. They say, "Why is this person at this organization that I have never heard of taking a look at my data?" And so, if I was going to think about this in a stepwise approach, I think there are some technical pieces, but there is also some baseline understanding of and baseline education of all the ways in which my data is shared.

That might be a first step to getting there because I think when these conversations have happened in the past, part of that brick wall that has been hit was "Well, this is too complicated to do because patients are going to say, 'Why did this person have access to my data?' And they are not going to understand all the pieces of the infrastructure." I am interested in Anna's perspective on that, but if I was going to think about a multiple-step approach to get there, I might start with getting over that hurdle so that we can then get there in a multiyear framework.

Medell Briggs-Malonson
Excellent, a multiyear framework in order to step us forward, but again, making sure the awareness and knowledge of what the appropriate sharing and disclosure of data is versus what we would be concerned about. Thank you, Hannah. Anna, we will talk about that, and then go into the next topic, which is related to this as well.

Anna McCollister
The next topic is a thing that I have been talking about on different panels for more than a decade, and it kind of drives me bonkers. My first foray into health IT was a company doing big-data analytics of deidentified health record data. I think it is absolutely essential that we have secondary use of data in research; that is critical in so many ways. However, people need to understand how their data is being used, and by whom. I have been talking about this for a while, and I work with different clients. I got one of my clients to actually issue a data use transparency and impact report, which I have shared with this group before and am happy to share with it again. And the response from patients was one of excitement, to be able to see how their deidentified data have been used to advance research. The patients who took the time to read it were very excited.

So, if we want the ecosystem of real-world data and real-world evidence to thrive, it is important for people to really understand the many ways in which their data is being used. Having said that, I think there are probably a fair number of actors in the secondary data use world that would creep people out if they knew they were accessing their data, but that does not mean that… I think that makes it triply important that these types of transparency disclosures are essential. Again, I think secondary data are essential. HIPAA gives a lot of latitude to take data, deidentify it, and sell it. And I am all for a market, because unless you have a

good market for data, you are never going to get data that is in any kind of shape to make sense from an analytical perspective, but that needs to be disclosed.

We have a responsibility to individuals from whom that data originated to disclose how their data is being used, and by whom, and it is not something that is not doable. The education will not happen unless the disclosures happen, so if we wait until the education is done, first of all, nobody is going to care that much in terms of patients. It might be moderately interesting, but they will not care after they see how their data is being used. But if companies are concerned about how patients will react when they see how they have used their data, they will come up with educational materials. But if you wait for the education to come before the data transparency is done, it is not going to happen.

Medell Briggs-Malonson
Thank you, Anna. Is it the chicken or the egg right now about what we need to do? But we all recognize the importance of education and transparency, and we want to make sure that we are equipping our patients with all the knowledge that they have. Anna, your comments were perfect to go directly into this, and you already commented on the transparency and use of deidentified data and provided your insights. I wanted to formally go through this topic and see if there are any other additions to it. Once again, the gap here is that patients have limited understanding and transparency into how their deidentified health data are shared. We already started this conversation with Anna, Hannah, and Deven. There is currently no consensus on how to provide patients with a description of how deidentified data are shared, and the opportunity is to learn more about patient preferences for disclosures about the sharing of their deidentified data. And it may also be that making sure, again, that we do have the appropriate education is another opportunity.

I have already heard some other proposed recommendations, but the ones right now are to explore patient preferences for disclosures about the sharing of their deidentified health data and explore opportunities to encourage healthcare organizations to regularly provide increased transparency into how to use identified data as well. Again, as everyone said, it does kind of flip back to even the past one, because even the proposed recommended HITAC activity for the first topic on the page is to recommend a simplified model of not only accounting, but also likely the education to also support the awareness for a patient. So, any additional comments on this topic, the transparency and use of deidentified data? I see lots of comments going on in the chat right now, too. Ike, I see your hand.

Steven Eichner
Not only patient preferences for disclosures, but patient preferences in their role in making disclosures or approving disclosures are also important. What is the patient role in actually making determinations about when and how their data is shared?

Medell Briggs-Malonson
Correct. Ike, you were going out just a little bit at the very end, at least on my end, but also the role that providers should play in terms of increasing that transparency. Is that what the comment was?

Steven Eichner
Yes.

Medell Briggs-Malonson
Great. Thank you, Ike. Any other comments or thoughts?

Anna McCollister
I would just add that I would caution us against trying to come up with ways for patients to approve disclosures before we do transparency, just because it is going to make it really, really complicated and is going to slow down transparency. So, I think the demand for the ability to choose whether or not your data is disclosed can come after the transparency, but if we try to do them both concurrently, we are never going to get transparency.

Medell Briggs-Malonson
Anna, can you do me a favor? I just want to make sure everybody is clear, especially for the record. When you say "transparency," can you explain what you are referring to in terms of transparency? I think it has some additional insights and implications.

Anna McCollister
I can share again the data use transparency and impact report that my client put out because I think it is a great example of how it could be done. In that case, it was an overview of both internal and external uses of deidentified patient data. In this case, it was a genetic testing company, and they used their data internally to do a number of things, such as improving algorithms, etc., but externally, they shared it, used it for research, and allowed others to use it for research, and in that case, it was a list of all the research that had been generated from deidentified patient data. I anticipated that this would be the case, but patients responded very positively to it because it was a lot of incredibly important and compelling research.

So, that is the kind of thing that I am… Based off the way that my insurance company is now approving certain medication requests from my physicians, they have access to my data that is identified. Somewhere along the line, I consented to that, but I have no knowledge of that, other than the fact that, suddenly, they are approving things that they have fought me on for years. But if LabCorp is sharing data with my insurance company, they need to disclose in some sort of an annual report what companies they share our data with.

Medell Briggs-Malonson
Right, and why.

Anna McCollister
Correct, yes. Is it research? No? In which case, awesome, that is great, do what you want, but tell me. Be up front about the companies with whom you have relationships that you are sharing my data with so that I can know.

Medell Briggs-Malonson
Absolutely. Thank you for that clarification, Anna. We have to move to public comment, so, Rochelle and Hannah, I know you have your hands up, but we are going to have to move to public comment. You are welcome to put it in the chat. If we do have one or two minutes, then we will definitely come back for very short wrap-up comments, but I will turn it on over to Peter so we can start public comment.

Public Comment (01:22:31)

Peter Karras
Great. Thanks so much, Medell. At this time, we would like to open the meeting for public comments. If you are on Zoom and would like to make a comment, please use the hand raise function, which is located on the Zoom toolbar, at the bottom of your screen. If you are just joining by phone only today, you can press *9 to raise your hand and get in the queue. Once called upon, press *6 to mute and unmute your line. I will pause to see if there are any hands that are raised on the Zoom. I do not see any. Just a reminder that all HITAC meeting materials are posted on HealthIT.gov. I am not seeing any hands raised, and there are no comments through the phone at this time. Medell, I can yield the time back to you.

Next Steps and Adjourn (01:23:25)

Medell Briggs-Malonson
All right. Thank you, Peter. So, if we can do rapid-fire, meaning 30 seconds or less, we can get some of the last comments in. Hannah or Rochelle, did you want to do a quick rapid-fire?

Rochelle Prosser
Rapid-fire was my thoughts in the comments, and I want the public to understand that I am not necessarily looking at it from a punitive aspect. Sometimes, you need to say, “Okay, we hold the purse strings. If we do not do this, then we will cordon off a portion until you do so and educate the public on that aspect.” So, I was just talking about if we are in the right genre or space to do so when discussing that. Thank you for your time, Medell.

Medell Briggs-Malonson
Thank you, Rochelle. Hannah, I saw that you put in your comment. Do you want to have the floor to explain that? We have about a minute or so.

Hannah Galvin
Sure. I was just going to note that more sweeping privacy legislation in the European Union (EU) has enabled more transparency, as well as the right to say, “I do not want my data shared anymore in this way with this entity.” But that is more sweeping outside of just healthcare data, so there is some precedent for this here. I know more sweeping privacy legislation has been proposed here in the US in different venues, but I would be interested, and maybe we can bring that back and ONC can update us on if there is any sort of proposal around this because I think that might be relevant to what we are discussing here as well.

Medell Briggs-Malonson
Absolutely. Thank you so much, Hannah, and thank you to the entire workgroup. We only have one more topic to go through during our next meeting, and then we are also going to prioritize all of the various different topics based off what we think has the greatest urgency right now versus some additional time in order to think about a potential multiprong, multiyear approach. Once again, I want to thank everyone for all of their inputs and perspectives. If there are any additional ideas, please feel free to email us, as well as Michelle. We are happy to incorporate your various different thoughts. Our next meeting will actually be on the 26th of August, but we will present the crosswalk ideas at this upcoming HITAC meeting. Once again, thank you, everyone. Enjoy the rest of your summer, and we look forward to seeing you all next week as well as at our next meeting. The meeting is adjourned. Have a great day, everyone.

Anna McCollister
Bye, everyone.

QUESTIONS AND COMMENTS RECEIVED DURING PUBLIC COMMENT

No comments were received during public comment.

QUESTIONS AND COMMENTS RECEIVED VIA ZOOM WEBINAR CHAT

Deven McGraw: Happy to be here!

Anna McCollister: FYI - Anna McCollister is here. Sorry for running late.

Eliel Oliveira: Thanks Hans. I unfortunately have to also leave at 1p.

Rochelle Prosser: +1 Steve

Eliel Oliveira: +2 Steve

Rochelle Prosser: +1 Medell

Eliel Oliveira: Yes, for Admin AI!

Rochelle Prosser: There are providers in the Indian Health Service as well.

Steven Eichner: And AI for public health purposes- there are very interesting opportunities for the use of AI to support different public health needs and reducing the administrative burden on reporting entities.

Steven Eichner: Accessibility to AI tools is important not only in terms of making technology accessible to indices with disabilities but also in terms of technology access in rural and other underserved communities/environments.

Rochelle Prosser: That is fine. The providers are found within those scopes of the context I provided. Do not want to provide a barrier to care since AI is not going away. but there are aspects of care to which we will make suggestions that we cannot make a blanket statement unless we bring those concerns in a legal inclusive framework. We must remove the barriers found now to providers who care for those populations I mentioned.

Eliel Oliveira: Good point Hans

Rochelle Prosser: +1 Hans

Rochelle Prosser: +1 Deven

Hans Buitendijk: Deven: Thank you for clarifying that!

Hannah K. Galvin: Agree, Deven!

Hans Buitendijk: While we may not need to have alignment on a single set of sensitive data for each context, for IT to be able to assist in managing we must have clarity on the superset of sensitive data/flags that privacy rules and consent directives are applied to. Particularly when sharing the data there must be continuity of meaning and purpose so a patient's data set is managed consistently.

Eliel Oliveira: That is the kind of clear definition I feel we do not have Deven! Just what you said about notes is very helpful.

Rochelle Prosser: Thank - you for this clarification Deven. I agree as well on the part 2 of the rules.

Medell K. Briggs-Malonson: Hans, I agree. I am concerned about lack of consistency of what data should be handled with greater sensitivity. I also agree with Deven with being thoughtful about these approaches.

Rochelle Prosser: +1 Steve

Eliel Oliveira: +2 Ike

Rochelle Prosser: +1 Hans

Hannah K. Galvin: Here is a state by state reproductive health law report: https://cdt.org/insights/report-two-years-after-dobbs-an-analysis-of-state-laws-to-protect-reproductive-healthcare-information-from-interstate-investigations-and-prosecutions/

Medell K. Briggs-Malonson: Thank you Hannah.

Deven McGraw: Another area is adolescents 😳

Rochelle Prosser: +1 Deven, I think it is a repeat of my comments from the prior rule recommendation.

Eliel Oliveira: Apologies to all that I have to leave in a few minutes (12p CT). What a great and important discussion and really appreciate everyone's comments and thoughts.

Deven McGraw: Data holders/sources (and potentially HIEs working on their behalf, depending on their model/capabilities) will each need to have the capacity to respond to the laws that apply and the needs of their patient populations. That feels like the right place potentially to start. Give providers the tools to protect data - and then some hope of notifying any recipients of the data of any applicable sensitivities/protections - perhaps is where to start?

Rochelle Prosser: I worry that with granular focus will provide pathways to unique challenges to the rule or specified populations for punitive data capture.

Hannah K. Galvin: @Rochelle, could you provide more context?

Rochelle Prosser: Hanna I hear you and agree. But I am concerned with the unique use case challenges that a broader blanket will provide coverage.

Hannah K. Galvin: Not sure I understand what you mean by a "broader blanket," @Rochelle - could you please clarify?

Eliel Oliveira: Thank you all. See you in our next call.

Hannah K. Galvin: Just to clarify about TEFCA, I see this as a stepping stone - agree, Hans.

Deven McGraw: If we consider this issue as giving providers, through certified HIE, the tools to flag/protect data that is sensitive, we don't have to define it and each provider can operate consistent with the needs of its patient community.

Hannah K. Galvin: Agree - the goal is to provide flagging capabilities; as well as some administrative tagging capabilities based on the legal landscape.

Rochelle Prosser: +1 Hans

Hannah K. Galvin: @Rochelle - I'm still not sure I understand your example, but happy to follow up offline.

Hans Buitendijk: Flagging where the data set / document contains that, or knowing the data (codes, values) on the individual data. Plus context where the combination of data yields sensitivity (the hardest one).

Rochelle Prosser: Yes, I am happy to do so. @Hanna

Steven Eichner: The disclosures should include TPO disclosures.

Rochelle Prosser: So who is responsible in these external organizations to notify the members of who is accessing or which departments are sharing their data. Sometimes transparency can shine a light on process and protocols that are meant to confuse the public.

Deven McGraw: Rochelle, no one is required to do this today, at least not under the HIPAA regulations.

Deven McGraw: I'm a big fan of this recommendation - but I'm struggling to figure out whether any agency within HHS has the authority to do it — other than CMS making it a condition of participation or a payment condition….

Rochelle Prosser: If we are to advance these necessary issues to action, we need to address this to bring forth transparency. The fact that it is too hard, complicated, should not be the barrier to move proposals forward.

Rochelle Prosser: Well this can become an information blocking situation. Maybe this is not the right forum. I do not see this as being an issue. transparency as education as a condition of participation. it is 20 years too delayed.

Rochelle Prosser: Devon you bring up a great suggestion.

Deven McGraw: Covered under payment - your consent wasn't needed, Anna.

Deven McGraw: (Per HIPAA)

Deven McGraw: Or Operations.

Shila Blend: Agree Anna

Hannah K. Galvin: I was just going to say that under GDPR (which is for consumer data protection, not just health care), the EU has successfully enabled this type of transparency as well as enacted the right to erasure - so there is some precedent for this. One question I would have is whether more sweeping privacy legislation may be in the works.

Anna McCollister: FYI - I'm having vision issues, so I'm having a difficult time reading the chat. Let me know if there's something specific directed toward me.

QUESTIONS AND COMMENTS RECEIVED VIA EMAIL

No comments were received via email.

RESOURCES

AR WG Webpage
AR WG - August 5, 2024, Meeting Webpage

Transcript approved by Seth Pazinski, HITAC DFO, on 8/26/24.