Transcript

HTI-1 PROPOSED RULE TASK FORCE 2023 MEETING

GROUP 2: ONC HEALTH IT CERTIFICATION UPDATES – NEW AND REVISED CERTIFICATION CRITERIA

May 24, 2023 10:30 AM – 12 PM ET

VIRTUAL

Speakers

Name	Organization	Role
Steven Eichner	**Texas Department of State Health Services**	**Co-Chair**
Steven Lane	**Health Gorilla**	**Co-Chair**
Medell Briggs-Malonson	UCLA Health	Member
Hans Buitendijk	Oracle Health	Member
Jim Jirjis	HCA Healthcare	Member
Anna McCollister	Individual	Member
Deven McGraw	Invitae Corporation	Member
Aaron Miri	Baptist Health	Member
Kikelomo Adedayo Oshunkentan	Pegasystems	Member
Naresh Sundar Rajan	CyncHealth	Member
Fillipe Southerland	Yardi Systems, Inc.	Member
Sheryl Turney	Elevance Health	Member
Michael Berry	Office of the National Coordinator for Health Information Technology	Designated Federal Officer
Sara McGhee	Office of the National Coordinator for Health Information Technology	ONC Program Lead
Mohammad Jafari	Individual	Presenter
Elisabeth Myers	Office of the National Coordinator for Health Information Technology	Presenter

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

Michael Berry
Good morning, everyone, and welcome to the HTI-1 Proposed Rule Task Force. I am Michael Berry with ONC, and I would like to thank everyone for joining us today. I would also like to thank our guest presenters for joining us today. We appreciate the participation. All of our Task Force meetings are open to the public, and your feedback is welcomed, which can be typed in the Zoom chat feature throughout the meeting or can be made verbally during the public comment period that is scheduled towards the end of our meeting this morning. I would like to begin rollcall of our Task Force members, so when I call your name, please let us know if you are here, and I will start with our cochairs. Steven Lane?

Steven Lane
Good morning, and welcome, everyone.

Michael Berry
Steve Eichner?

Steven Eichner
Good morning, and welcome.

Michael Berry
Medell Briggs-Malonson?

Medell Briggs-Malonson
Good morning.

Michael Berry
Hans Buitendijk? I see Hans on, but maybe he is muted. Jim Jirjis?

Jim Jirjis
Present.

Michael Berry
Anna McCollister? Aaron Miri? Kikelomo Oshunkentan?

Kikelomo Adedayo Oshunkentan
Good morning.

Michael Berry
Naresh Sundar Rajan? Fil Southerland?

Fillipe Southerland
Good morning.

Michael Berry

Sheryl Turney?

Sheryl Turney
Good morning.

Michael Berry
Hi, Sheryl. Thank you, everyone. Now, please join me in welcoming Steven Lane and Steve Eichner for their opening remarks.

HTI-1 Proposed Rule Task Force Charge (00:01:30)

Steven Eichner
Good morning, all, and welcome to this Group 2 Task Force meeting for May 24th. We have a really good agenda put together for you where we are going to have some great presentations on patient-requested restrictions on certification criterion and data segmentation for privacy and consent, and if we have time, we will spend a little bit of time looking at our worksheet. I do want to extend a special welcome to members of the public. We will have a public comment period towards the end of our meeting. You are welcome to contribute things electronically to chat, and when we get to public comment, there will be opportunities for us to address comments, either through the chat interface or we can open up phones for live questions or live suggestions. Steven, do you have anything to add?

Hans Buitendijk
May I do a quick sound check to see whether you can hear me now?

Steven Lane
We have you, Hans. I was on mute, however.

Hans Buitendijk
Now mine is working too. Okay.

Steven Lane
I just wanted to add my welcome to Ike's. I will be trying to monitor the chat as we go along, and I really look forward to a rich discussion.

Steven Eichner
Before we get into our content, we are going to do a quick review of our charge and the scope for the Task Force overall and this particular workgroup, so let's go to the next slide, please. I will not read it, but again, just as a reminder, our general charge is to provide feedback to ONC through the HITAC full committee on the HTI-1 proposed rule, and there is a list of specific charges of specific items that ONC is looking for feedback on particularly, and those are available in the slide deck for your perusal. All information for meetings is available on the ONC website for members of the public. Next slide, please.

So, looking at today's meeting, we are focused on patient-requested restrictions and data privacy, so let's go through to the next slide, which highlights our focus. So, I think that is all we have for a quick overview, so I would like to shift to our next slide and welcome Elisabeth Myers, who will give us a presentation on patient-requested restriction certification criterion. Elisabeth, the floor is yours, and welcome.

Steven Lane
Beth, you seem to be on mute.

Patient Requested Restrictions Certification Criteria (00:04:56)

Elisabeth Myers
My apologies, sorry about that. I was trying to check in on who else was on from ONC, and I think it is just me for this presentation. So, let's get started. This is a new criterion that we proposed in the proposed rule that was recently published, obviously, that you are all aware of and are working to review for us. I will say that before we dig in, for those of you who have been on the FACA for a while or paying attention, this is not new news for us, although this is a different way of thinking about some of the technologies that we have previously adopted and trying to think about ways we could build on them and build on the standards that are already in the program to try and advance additional parts of this very complicated space of managing consent, persistent consent, and thinking about different ways that privacy constraints can or should potentially be supported by health IT to replace manual processes that are either burdensome or ineffective.

So, that is really a broad intro impetus behind this, and we can dig into the slides now. I apologize ahead of time that they are very text-heavy. We put a lot of information into this very short section of our reg, so it is going to take a little bit to get through some of these nitty-gritty details because they are what we want you to focus on. There are specific questions about variations in the use of potential standards and variations in the functionality that we are, in particular, interested in hearing your feedback on. Go to the next slide. This is our little disclaimer. You all have seen this over and over again, especially over the past few weeks, so we can move on.

So, this is the summary of the proposal. Again, I apologize, there is a lot of text. Hopefully you all have your reading glasses on, as I know I do, and we can talk through what we have proposed within the rule itself. So, there is an important cross-reference in our regulation that I am going to highlight first, even though it is in the middle of the bullets on the right-hand side, and that is the HIPAA privacy rule and the right to request a restriction on uses and disclosures. This is a really important thing that already exists within HIPAA and is foundational for the concepts that we are trying to think about health IT supports to enable. The reason for that is we recognize that as we work together to advance the types of data that are available, there are always risks associated with that.

You have had the presentation on DSI previously, and it had the same sorts of questions and considerations that, as we advance technologies, we need to be thinking about how those technology advancements could have negative impact on different patient populations and different communities, especially when we think about things like what we are adopting for USCDI Version 3 and how individual community members or individual patients may identify some of those new data elements that are critical to their care as also being sensitive data, and what we have tried to do with this particular proposal is not define what we think sensitive data is or should be, but instead, identifying and recognizing the concept that that may well be fluid, especially for individuals who have faced discrimination or for whom there is historic discrimination inherent in our institutions, and that there may be considerations they have that they personally want to be able to have more control over certain restrictions, but do want the data to be able to flow for the purposes for care where and when they want it.

So, that is what we have really focused on. That is why you will see that there is not a definition of what "sensitive data" means. We have explicitly noted that it is under what the patient may view, and we are relying on that construct in the HIPAA privacy rule right to request a restriction to help set that parameter that this is about patients' choice and patients' rights for those types of restrictions on particular uses or disclosures.

So then, moving back to the left-hand side, what we have proposed from a regulatory point of view as a starting point, though you will see that we are going to get into some alternate proposals as well, is that the primary proposal is that a health IT module that fits under a certain set of interoperability data must view a functional criterion, must certify to a functional criterion, which is the D14 you see up at the top, for any of the data expressed in 172.13. Sorry for the reg references again, but that is the USCDI. So, for any of the data expressed in the standard that is defined by the USCDI, and that does mean USCDI Version 3, a health IT developer must enable a user to "flag" for whomever such data needs to be restricted from being subsequently used or disclosed and prevent the data from being included in the use or disclosure based on that potential flag.

We propose to modify the privacy and security framework. For those of you who are familiar with the reg structure, that is the suite of privacy and security criteria that sort of stand on their own, and then, within that framework, it tells you which criterion needs to have those privacy and security pieces applied to it in order for it to be certified in the program, and so, that is sort of how it works, that it layers these privacy and security framework pieces on top of existing criteria for specific purposes. So, we have added this new privacy and security criterion to that framework, and then, we have also added a different functionality, and this is a little bit different.

We have done two pieces here. One is allowing a user to have the capability to do this particular piece of identifying where there has been a patient-requested restriction, but we have also done something with what we all colloquially call the view/download/transmitter, the patient portal functionality, to add a capability that there must be an internet-based method to request a restriction to be applied in that functionality as well. That is not totally out of nowhere. We have done these internet-based methods in that criterion in the past for things like requesting a correction or requesting review, so it is in that same suite and we thought it might fit in well there, but again, that is a question we have for public comment and that we would love to hear from you all. So, let's move on. We have a lot of detail to get through.

So, we have tried to set some parameters to give us a starting definition. You will note that what I just described to you is all standards agnostic with the exception of the USCDI, and there is a reason for that. Our original consideration of this was trying to figure out what can and cannot be supported by standards, and there are pieces that are supported by existing standards, either that we have already adopted or that are very similar to those we have adopted and are in other aspects, for example, the FHIR data segmentation for privacy, for which we are going to have a presenter talk a little bit more about after I finish, but what we have tried to do is do a functional criterion to start with because what we are trying to figure out is that piece where you are actually enabling that piece of the patient to make a request, which is that patient portal piece in that E1 that I mentioned, but also the user to actually create the action that is associated with the "flag," and that is not necessarily fully supported by the IGs as they exist currently, and

so, it is something we are trying to figure out how it would work, and we ask a lot of questions in the rule about that.

What we have said specifically, though, is that enabling a user to flag means enabling the user of the module to indicate that a request for restriction was made by the patient and that they intend to honor that request, and that is a two-part indication that is important to keep in mind. There is user discretion under the HIPAA security rules about honoring that particular request, so it is not an automated process where a patient makes a request, it goes through, and there is no checking on that. It is intended for the user of the health IT, which, in many cases, will be the healthcare provider or an administrative representative at a healthcare provider.

So, the request made by the patient could be automated. In other words, if the patient does the internet-based method, that could be presented to the user to either approve or not, but what we are really trying to get at is what we have heard from clinicians and providers, that right now, they do not even have a way to indicate that a patient request has been made, and that is part of what we want to allow for, is that that request might be made via other means. They might make a phone call, send a letter, or some other request method that they might actually ask the user to consider, and we wanted to make sure that this criterion, from a functional point of view, is also considering that. Again, there is not necessarily a standard that accounts for that "request made" portion of a consent or privacy disclosure request.

So, the last piece is that what we are trying to do with this, given the gaps in what is existing in current IGs in terms of how that initial request is captured, and then, what happens next, is that in the primary proposal, we have not proposed a standard for that, so the flexibility to implement and enable a user to flag could be in a lot of different manners depending on what the developer things is most appropriate and most effective. From there, we go to the next slide. I think I need to talk a little bit faster. I am just trying to get through all of this and still have room for some questions.

So, I have already mentioned the standards-agnostic approach, but I have provided more detail here so that we can really be laying out for you what we want you to think about and look at. The first proposal, the primary proposal, is a standards-agnostic approach, and the reason for that is, again, we know this is happening in a lot of different ways currently, and developers have been thinking about a lot of different ways to try and support these types of workflows, and, as mentioned, without a clear IG that actually includes these pieces of it, there is not a lot of consensus on what is the right way to do it, and so, our concern is that, frankly, we do not want to get that wrong.

So, we have a done a standards-agnostic approach that allows us to provide flexibility in implementation for developers to think about how this could be implemented. Again, such flags could leverage the existing standards like DS4P, implementation guides, or some of the subsets within them that we talk about a little bit more in the alternate proposals, but our primary proposal would not be requiring these to such standards for this particular criterion. I do want to mention that we do have two other criteria in our program right now that do use those standards and do require the granular level for them to actually apply and/or recognize security labels, but the concept of including that with a provider mechanism to recognize the patient right to request a restriction is where, again, there are gaps in how that actually works.

And then, finally, there is a gap in how the action is implemented. For example, those IGs all include instructions, but they do not actually include how you do that instruction. They say an action like "not for redisclosure" or "redact," or they may say layers of actions, depending on how the different pieces of the IG fall together, but it does not actually say what that means in the real space in terms of how that could be implemented. I know a lot of you all and a lot of others in the health IT and healthcare community are working on all of that, so we are trying to keep this flexible so that those approaches could be part of this proposal or part of this criterion, and it could recognize that fluidity and that flexibility until we call can sort of move together toward consensus of how these actions should be addressed. Next slide.

So, these are the alternate proposals in a request for information, and this is a tool that we have used in the past in our regulations. Some of you may be familiar with when we were adopting FHIR in the first place, we were not sure where the industry would be in terms of which version would be most appropriate and which supports would be most appropriate, so we used a similar approach where we proposed one concept as what we think might work and we proposed alternates so we can actually have a clear idea and provide some clear questions for the public to give us clear feedback on whether the primary proposal makes sense or one of these alternates would be better, what interplay there is, and what could work best. So, we propose several alternate proposals that are aligned with standards that we have already adopted or standards that are very similar to standards we have already adopted, and the important part for some of these is that these are for the D criterion.

These adopted standards of aligned alternate proposals are not for the view/download/transmit capture. Again, there is not a clear indicator of an IG that could be used for exactly that purpose, so we have left that one without doing an alternate proposal on a standard. So, the alternate proposals are doing a layered set of things, and hopefully, we have made it clear enough in the reg that it is easy to understand how we have done it. We set one where there is an alternate proposal where we would adopt the full scope of the DS4P IGs, and that is both of them. One is the DS4P IG that is already existing for C-CDAs, the other is the DS4P IG that is existing for FHIR. They have slight variations, but both use the HTS security label vocabularies, and that is what we would be referencing within the alternate proposal as the scope of the type of flags that would be applicable.

To be clear, reminding everybody that those are the flags, and again, there is a set of instructions that goes with each flag, including the general purpose or what the restriction is, and then the **[inaudible] [00:20:14]** action or the action that is supposed to be taken with that applicable thing. So, in adopting those IGs in whole and the security vocabulary, it is adopting the whole suite of all of those pieces, so that is what that proposal is taking a look at. Should we look at those IGs and use them at least as a vocabulary for the tag, for the purpose, for the workflow, and for the action that is identified, keeping in mind that that would mean that there is still a gap in that the action is identified and there is not an IG that actually says how that action that is identified is implemented. In other words, how is the redaction implemented? How is the "do not reaggregate/do not relink" implemented? So, there are some outstanding questions there, and we include them in what we are covering there as well.

Then, the second alternate proposal is to take those same IGs, and recognizing that those IGs include a vast suite of potential security labels, potential purposes, and potential actions that go well beyond what the HIPAA right to request a restriction actually defines and sets in scope. For instance, there are tags in there that relate to things entirely unrelated to the patient's preferred choice. For example, you could do

something with a Part 2 purpose, a Part 2 consideration, or a state privacy law. There are different ways that they capture those that would be different than the patient's request. So, a second alternate proposal asks the question of should we use the HTS security rule vocabularies, but then apply constraints to them beyond those described in the IGs that would align the vocabularies for the purpose, for the requester, for the requested action, to only the use cases that are aligned with the HIPAA right to request a restriction, and questions and our rationale for considering that particular alternate proposal is that we recognize that, to some extent, all of these things are still squishy in terms of how they get implemented.

We know a lot of people are working very, very hard to move things forward for individual use cases, but as we mentioned in the CURES Act final rule, even the use of security labels and how they get persisted, our focus for that rule was thinking about pediatric and opioid use cases. Yes, the full scope of the IGs is applicable, but it is a capability to use those labels, whereas this would be not only a capability to use those labels, but to specifically act on them, and recognizing that the action that we are talking about is the HIPAA right to request a restriction, and that is the patient-directed request for sensitive data restrictions. The IGs themselves include a much broader suite, so we are trying to balance not making that full suite required for this particular purpose so that we can focus in on the patient right to request a restriction use cases and see if we help do advance that through this targeted focus for the certification criteria.

I realize that that sounds a little convoluted, and I hope that you will all bear with me and take a look at the actual questions so you can sort of get an idea of why we are considering that because if you look at the full permutations of those IGs, it includes a lot of other use cases, and we are concerned that the requirement not just to provide a capability for labels, but provide the capability to actually implement the action is where they would become difficult or potentially even impossible at this point in time, so we are still trying to think about how we can move forward with something that might be readiness without constraining the ability to do the particular action that we are looking at for this particular case, and I did see in the chat that there is a question looking at FHIR path. We are actually looking both. The current proposals all include both FHIR and document-based exchange, as well as the patient portal, so we are covering our bases there to try and cover all of the current use cases where such a transaction might need to be applied in order to honor those types of requests.

So then, finally, our additional alternate proposal is similarly trying to consider is this too broad, is this too big, should we look at the USCDI and not include the full set of USCDI? Should we zero in and, again, not fully defining what "sensitive data" means, given that this is about patients' rights to request a restriction, that thinking about where are the pieces within the USCDI that we have heard from patient advocacy communities already might be, in particular, related to sensitive data, related to stigmatized care, related to historic and potentially institutionalized discrimination.

And so, for those particular items of the USCDI, we did an alternate proposal zeroing in on where we think those types of data elements fall based on the feedback that we have had from patient communities and saying should we restrict this particular implementation, this functionality, to tagging and acting on tags for just a subset of USCDI, trying to keep this within scope and make it a little bit more feasible? Again, throughout this entire proposal, you will see cases where we are saying we think this is very important, but we very realistically understand that this is a major challenge and incredibly complicated, and we are trying to figure out if there is a way to move pieces of this forward together in a way that is feasible and actionable,

and we very realistically want to hear your feedback on what is or is not feasible, what may or may not work, and if there are additional constraints that we should consider. Go to the next slide.

So, with the alternate proposals/considerations, this is going into a little bit deeper purpose behind why we have done these alternate proposals. As mentioned, our primary proposal is the standards-agnostic approach, and again, I mentioned the reasons behind that. We think this is happening in lots of different ways or, in some cases, not at all, and there is a lot of work still trying to figure it out, so we want to try and allow that to flourish and help to further define where those gaps in the IGs could be filled with clearer consensus-based standards approaches, so that is our primary proposal, but we do think that there could be some value to leveraging what is in the IGs to help set some parameters or some guide posts, so we believe that those alternate proposals, which rely on those standards, may be preferable for developers, but we want to hear that. If that is the case, please let us know, and if it makes sense to constrain them or think about different constraints from what we have included, we would also like to hear that, and that transitions me to my last slide.

There is an extensive set of requests for information in this particular section of the rule, given its length. You will see in the alternate proposals themselves that there are questions on every single one. There are questions on each piece of the primary proposal asking is this the right way to do this, is this something we even think of, how does this work, what does the burden look like, what is the potential value or benefit, what do the alternative constraints look like, but we have also included a specific set of questions that relate to the alignment with other applicable laws. So, our intent and our starting point for this particular case is thinking about patient request for restriction and the existing right under the privacy rule to request restrictions for certain use cases and disclosures, and again, I refer you back to those sections for all the questions that relate specifically to each of those proposals, each of the standards associated, and so forth, but we also recognize that that will not discharge the full workflow for the HIPAA privacy rule, including things like which disclosure purposes or other types of permutations go with the privacy rule for it.

So, we are trying to be clear that it does not discharge the full action, it is just this piece of the workflow that we have focused on, and that we are trying to understand if we got that right and if doing this tool would be useful to try and help move some of the pieces forward within the HIPAA that are not currently supported by standardized health IT. However, we also recognize that there are other additional applicable laws that are potentially challenging, to say the least. As noted, we previously talked about pediatrics and opioids, and there is Part 2, and there are varying state laws for all different types of information.

As everybody knows, that is continuing to become more and more complex, and so, what we are asking in this particular section is if there are additional applicable laws that affect the exchange that we should consider when we are trying to think through what a certification criterion health IT supports might look like, and this does include a cross-reference to the information-blocking provisions that we have been talking about, where we are thinking about is there a tool that could allow patients to have more dynamic requests in terms of when they want to see specific data or what types of information they want to have disclosed to them prior to a conversation with a clinician or after a conversation with a clinician. We recognize that this functionality as we are proposing it is trying to zero in on a slice of these use cases, but we are also asking questions about is it appropriate, should we consider other things, are there ways that this functionality could be more broadly used if we modified how we are proposing it.

So, there are a lot of questions here, and I realize I just took up more time than I originally intended to get through the detail level, but hopefully this helps to provide you some context that you are considering further and thinking through what your recommendations may be for how we approach this, what we do with each piece of the puzzle from the criterion point of view, and if there are additional puzzle pieces that we should consider in a certain or specific way. We very much want to get feedback on how this could potentially work. So, I will pause there, and I think I am passing back to Mike. Are you managing the questions?

Michael Berry
That would be your cochairs.

Steven Eichner
Ike and Steve Lane are managing questions. There is a lot of active discussion in the chat. I do want to open the floor for any questions from Task Force members. If they would like to raise their hands, we can acknowledge folks that way as well. Jim?

Jim Jirjis
Listen, I totally endorse the patient's ability to control sensitive information. My question is more about the feasibility given the current state of the data. So, if your patient is maybe not that sophisticated with how IT data models work and how the EHR works, and let's say you view HIV, which is something that you want to restrict people knowing about. Well, right now, even within USCDI, that may appear as a lab result and various different types of lab results. It might appear as a progress note in a narrative, or it might appear on the problem list or the med list, so I am just curious about patient expectation that they have actually restricted something when they really haven't and how feasible it is that that unintended consequence may occur.

That was one, and then, the second one was really about the ease with which people are able to do this. Obviously, I am in support of patients being able to restrict information that they want to, but for those who misuse it, how do we handle, first, patients who want to reverse it, as there is nothing in here about reversing something they have flagged, and second, the unintended consequences of a very incomplete record that may occur from overuse? So, the first question is feasibility and the second is about unintended consequences of safety of care. Did you guys consider those?

Elisabeth Myers
Those are very good questions. The first question, on the feasibility, I will say out loud that I think that is exactly the type of thing we are hoping to hear from all of you. We do specifically say almost exactly what you said, Jim, in the rule that there is a challenge here. The reason we included the whole scope of the USCDI is because that is the baseline in certification, and theoretically, anything within the USCDI could be sensitive, like a medication could potentially be sensitive, even for an HIV use case. So, if we think about it that way, that was our concern in the scope of this. It could theoretically be infinite, or at least very, very large, and very complex, and that is part of why, within the rule, we are trying to ask questions. Is there a way that we can move this forward, even in light of the extensive complexity? Because right now, we have nothing doing this particular piece.

There is not anything that is supporting a technical workflow to help make this particular process happen, and what we are trying to accomplish or thinking about ways to accomplish is can we do something,

recognizing that it does not solve the whole scope of the problem, so that is exactly the type of question that we would love to hear more of your input on, Jim, that we hear from you all what could we do if we can do something, how should we do it if we do something, and are we barking up the wrong tree if this is not the way to go about making a functionality that could begin to chip away at this problem, recognizing that the problem is huge, extensive, and only going to get more complicated.

In the proposal background, we talk about the USCDI, but what do we do when this starts expanding, thinking about genomics or patient-generated health data? How are we even thinking about whether those types of restrictions are going to be a privacy constraint? And that is something well beyond the scope of what HIPAA covers and well beyond the scope of what we can cover, but we talk about it because we think it is really important to set in context: Is this something where we can do a limited piece of the puzzle to try and help support a part of the workflow? Is that reasonable or appropriate?

And then, to your second question, I think we put a revocation in the patient portal piece. I will double-check that, so do not quote me on that, and if we did not, please provide us a note about that, but that is also part of eh reason that we left it pretty open, because the HIPAA right to request a restriction is not a blanket allowance. It does not say that the patient requests it, and therefore it happens. It is actually incumbent on the covered entity to make a decision based on the constraints of HIPAA whether they think that is appropriate. So, things like emergency restrictions or necessary for care are all considerations that already exist under HIPAA. All of that is already part of what is in HIPAA, so wee are actually not changing any of the existing requirements in terms of HIPAA and what HIPAA allows or does not allow from these restrictions.

Steven Lane
Hans, your hand is up.

Hans Buitendijk
Thank you, and I want to start with that this is an extremely important topic. I completely agree with a couple of comments made, starting with Beth, that this is only growing more as data is being shared, and we need to do something, so with a couple of other comments in the chat, can we focus on something incremental? As Jim is putting it, what is the feasibility and how does it work? Because as data is being shared, if we only focus on the source of the data and do some flagging, then where it is going to be shared needs to interpret that the same way and needs to act the same way, and the rules can change over time because today, I am uncomfortable sharing, and tomorrow, I will not be.

There were also good points as to what the data is in. Is it in notes, is it in a condition code, is it in a lab test, can it be implied? How is it transmitted, V.2, FHIR, CDA, proprietary, NCPDP, etc.? There are a variety of different mechanisms, and we have to therefore be very careful that as we embark on this, we really understand the expectations of what can we do initially and what needs to grow in over time, and be cautious that if we start to open too big, which is what the current standard suggested as alternatives would actually fairly easily lead into, having a variety of different ways of going about it, that that is actually going to set us off on the wrong foot. So, having something focused where we understand the principles, where we understand not only the flagging, but also the infrastructure by which we can enable that the data, however it flows around, which it actually flows around substantially and we are finding that 90% plus of

data is actually reshared with the same parties that originally shared it or that got it through other means. There is a lot of that going on. What if two sources come up with the same data with different flags, etc.?

So, I think we have to keep not only the flags in mind for the data that we actually use to evaluate, we have to be very careful that it is not just about flags, but as much as possible, it is about the data that is already being documented naturally, what we can use there, and the infrastructure. So, how can we carve that or focus that into a good first or second step? I would like to point back, and I am looking forward to some of Mohammad Jafari's comments in a moment as well, and indicate that actually, ONC has done some great work in that space by funding the LEAP Project, and there are other activities in place, so I do not think we are starting at zero, but we are starting at a point where we have lots of different good ideas, some standard, some practice, but we are trying to find that kernel in there where you can say that is the right start, and we can build from there based on that experience and get everybody involved in it, because only having a project here or there is not going to do it.

Allowing everybody to go off on their own is going to get divergent approaches, and I am very concerned that that is actually going to set us off on the wrong foot. As Jim Jirjis is also indicating, that is going to set the wrong expectations. You think the data is protected in that way and held private, but it is flowing through other means, it is interpreted in other ways, and it is still out there in a way that it is not intended to be, and that is a big concern.

Elisabeth Myers
Thank you, Hans. I will say I am glad that we record these because I think your entire comment should be submitted as a public comment on the rule.

Steven Eichner
Beth, this is Ike. I will take the next couple of questions for myself. I think we need to make sure that patient role and participation is really respected, honored, and part of the focus. So, looking at a patient authorizing disclosure or requesting the information not be disclosed is important, and looking back at the question of whether the provider is going to honor the patient's request, I think it is important that the technology support both noting the patient's request and then, as a secondary factor, whether the provider is going to be able to fulfill that request or not with a basis for if they cannot follow that request as to why not, PTO or other circumstance. Secondly, in that same space, having the ability to do it from a technology perspective as part of an IT module is one thing. Ensuring that that service is actually available in a findable way for a patient is a secondary, but very important component, so if the technology is built into the system, but a patient cannot find it or get to it, we have not really fulfilled the full scope of engaging the patient in choosing that role or choosing the data share.

Part 3 is looking at accountability, that if a patient requests that certain information not be disclosed, without accountability about what parts of their information are disclosed, the patient does not really have a way of seeing whether the provider has honored the patient's request and/or direction, so it seems to me that before we get too far down the path, as we are looking at developing some really good technologies in the ability to share information across providers, we should also be able to figure out a way of accounting for that way of accounting for that share or tracking that share and making information about that sharing available through patient portals, HIEs, or whatever so the patient can actually validate that their wishes

are being followed. I am not sure there is necessarily a response there, but I think those are important factors.

Elisabeth Myers
I was just going to respond and say you are raising a bunch of the questions that are exactly what we are trying to ask and think through, so, again, similarly to the response to Jim and Hans, exactly what you are saying is exactly what we are trying to understand and hear about, so I am really glad that this particular group is looking at this because I think your feedback is going to be essential to us figuring out what is the right thing to do with this particular piece, and as noted, we have a lot of permutations of that. I know we need to move on, and I am actually really excited to hear from Mohammad on his presentation as well, but each of the points that have been made are exactly what we are trying to hear and understand, so I just really appreciate your dedication and your volunteering to be part of this Task Force and help us think this through, and we really look forward to seeing the report the Task Force puts out in this particular piece, as well as that I know each of your organizations may individually be submitting public comment, and we look forward to trying to hear what you want us to try and do here. It is truly a collaborative piece.

Steven Lane
Thank you, Beth. The cochairs also look forward to workgroup members entering their suggestions and refining their suggestions in the spreadsheet. Hans has done some of that, as have Dayo and Sheryl, so we really want to get you in there. This is probably one of the most complex tasks that we have in our Task Force this year. So, with that, let's hand it over to Dr. Mohammad Jafari to give us a little bit more of the background on the current state of the technical standards and how we might be able to select from them to accomplish what we were trying to get at there.

Data Segmentation for Privacy and Consent (00:45:58)

Mohammad Jafari
Thank you, Steven, and thanks, everyone, for joining and having me today. I was reading through the chat, and I will try to address some of the comments that I noticed in the presentation, and hopefully there will be time to discuss things further afterwards as well. So, I will try to run through fast so we have more time for discussion. Thank you. Next slide, please. So, the first thing I wanted to note… I am going to start with some broad observations and then get to some specific notes about the state of current standards, and then hopefully conclude with some recommendations.

I want to recognize that there is a tight coupling between patient preferences and patient-requested restrictions and data segmentation. I think a meaningful way for patients to be able to actually articulate their preferences is to have data segmentation tags available to them, and to have that language to be used in the policy language to express those goals. I think this kind of emerged in the chat as well. It would be quite onerous for the patient to have to go through item by item. It would require a deep clinical knowledge to, for example, identify what medication line items would be sensitive and what would not, and what would lead to inference about certain conditions that are stigmatizing or are sensitive in the eye of the patient. So, in order to provide a meaningful language for the patient to articulate their preferences, we do need the sensitivity tags and the data segmentation in general.

So, I also want to raise this because I also noticed this in the chat. I think policy should not be persistent on data because policy changes. As was mentioned several times, people change their minds. They may

express a restriction and want to change it later, and I think this should be separated from the persistent attributes on the data. So, I want to refer to the FHIR consent resource and the audit event that provides hand in hand both the ability to articulate the policy, and, through a consent management system, handle revocation, updates, and changes to that policy would allow us to be able to enforce the policy without having to go back to the data and take a sweep at a large set of data because of a change in policy. I anticipate that the policy that comes from a patient, those preferences, is more likely to change than jurisdictional or overarching policies.

So, I think we need to have a cohesive view of both of these components, the consent management system and data segmentation, and there are some emerging standards on profile consent resource in order to identify those flags that are most common or most of use at the moment and most relevant, but I think the USCDI, for example, could also include a profile of the consent for this purpose. I do want to also note that it is technically possible at a rudimentary level to enforce patient preferences without really standardizing or requiring any standard data segmentation, leaving that all internal to the organization, but that would not be a method that would be an incremental approach to add these and more advance, sophisticated features in the future, and also, it would not lead to an ecosystem where more sophisticated rules that could be processed by recipients downstream could be expressed, articulated, and attached to data when data is raised.

One of those that I want to mention is to release data only through clinical decision support. So, if you want to capture obligations as sophisticated as that, like the patient is expressing to release the data, but not to the eye of individuals, but only to the decision support system so that that decision support system can enable warnings in case of patient safety so that a physician can actually call to break the glass, that is a sophisticated level of obligation that would require having data segmentation policy in place in order to be able to communicate these obligations in a standard and interoperable way. I do also want to note that the FHIR audit event that is part of the consent management system would provide an infrastructure for accountability, and also tracking what data was released based on what consents are authorized by what consents and provide the infrastructure for that sort of accounting of disclosure that was of interest in the chat and also in the previous comments. Thanks. Next slide, please.

So, I included this just as a sample architecture where data segmentation and patient preferences can play hand in hand. I think in a consent management system where the patient-facing UI allows the patient to articulate the rules, the language that they use in order to say, “I do not want to share anything that is related to reproductive health,” for example, should be consistent and connected with a security labeling system that actually identifies that sort of data, and that is essential in being able to enforce that. The other thing I want to note is that if we leave the data segmentation out of the scope for interoperability and within the organization, we might be able to enforce policy in a rudimentary way, just sharing but not sharing, but we will not be able to communicate anything further to the recipient in an interoperable way. So, in order to be stepping towards an incremental approach where we can actually add more value in the future, we need to be mindful of the fact that data segmentation is essential in having an interoperable ecosystem for communicating policy and handling instructions, basically. Next slide, please.

The next point I want to raise is the importance of labels themselves. Because the labels are the connective tissue for expressing granular preferences and patient-reported restrictions, it is important to have a consistent set of labels that are well-defined and are understood by all the parties. I think agreement on the

meaning and the semantics of the labels is important in order to make sure that everyone is actually going to enforce the policy in a consistent way. A minimal set of security labels that should be supported is important. We need to be mindful that what exists in the terminology is a very large data set of codes. There are a lot of codes in there. Some of them are outdated, some of them may be being replaced by a new code, and I think in order to at least keep the problem manageable and tractable, I think it is important to identify a well-defined set of security labels that are understood by the community and can be implemented to address the current and most germane use cases. Next slide, please.

I want to raise a particular concern and a challenge about sensitivity classes because sensitivity classes are not policy, they are rooted in the content of a resource or any data object. It is different, for example, to say, "I consider this confidential" or "I consider this resource a resource that should be volatile and should not be redistributed or has to be deleted after use" versus "There is HIV-related content in this data object," and because of that, there is a tight coupling between the semantics of sensitivity classes and the clinical content of the resource, and if the underlying clinical concepts are not consistent, if there is not a consistent understanding of what constitutes, for example, HIV or reproductive health, then there could be an inconsistent enforcement, like one provider may consider something to be one category, and the other may consider that to not be part of that category, and that could provide an inconsistent enforcement in the ecosystem. I think we need to determine whether this is an acceptable risk to take to allow innovation to build that technology for sensitivity tagging, or do we want to be more conservative and leave sensitivity tags out of the scope for this round of regulatory updates? Next slide, please.

I do want to note that currently, other than the SAMHSA value set that was developed many years ago, I am not aware of any other official implementation guide or any guidance or value set. There might be things here in the form of research from the academic community and otherwise, but I am not aware of any other effort to standardize the sensitivity classes and the clinical concepts behind the sensitivity classes.

Two final points. I think this was also raised by Hans. Data flows in different forms, and it is important to make sure that labeling, segmentation, and the enforcement of consent policies are applied consistently to all the gateways, and there is a need for a cross-paradigm framework. We do not have an individual implementation guide to harmonize everything across different specifications, but there is an implementation guide, as I will mention a little bit later, for FHIR, for CDA, and for V.2. I do want to mention that there is a need for having a harmonized view because these were developed separately and over different periods of time, and having a harmonized view to address all of these concerns in an implementation guide that addresses all of the paradigms is a key factor here. Next slide, please.

And then, I think everyone agreed that we need to have incremental implementation, and I think it is important both in order to, first of all, pace ourselves, create a stepwise plan where we can actually implement things and get more insight into what the next step looks like as we move forward, but it is also important to be able to certify things at different levels so that people who are looking to acquire products or buy services are also able to meaningfully understand what is the level of maturity for the capabilities that are implemented, and there is some emerging guidance on a maturity model and there have been whitepapers over the years, but there is no official implementation guide or certification on this at the moment. Next slide, please.

So, I tried to summarize some of the existing and emerging specifications and implementation guides. I think the HCS is sort of the foundational standard that defined the general concepts of security classification and privacy tagging, but it does not include any concrete implementation guidance and detailed implementation guidance, and I do not believe it defines the standard vocabulary, it just defines the structures, general categories, and types of data tags, but not the details. We have the CDA data segmentation for privacy implementation guide. It does refer to a standard vocabulary in text. There is some reference to both section- and document-level tagging, so it allows granular tagging beyond the scope of just the large CDA documents, and it does address how to model security labels in that sort of ecosystem.

FHIR data segmentation for privacy is a more recent version of the standard. It was released just about a month ago, and it does define a much more updated list and value set for codes and security labels of different categories. Again, it is referencing the terminology. The terminology includes a lot of codes. Some of these codes are referenced by inheritance-based, if you like, a parent code that is identified as the determinant for the value set, and there are a lot of codes there that may either not be clear to the community how to implement or the delineation between the semantics of Code A and Code B is not very clear, but all of that has been categorized and sort of formalized in that IG. It does mention a maturity model as a road map item, and there is some guidance on integration with consent and just general policy integration in that IG. There is also some non-normative guidance on implementation of the security labeling system, just general implementation notes in that IG. So, I think amongst the standards that were mentioned, this one is closest to be the most recent version and most updated understanding.

Version 2.9 defines the mechanics of recording sensitivity labels, confidentiality, and handling instructions, and also authorization policy. I am a little bit unclear about the data sensitivity labels. I was digging in this slide because I had a doubt about whether it is actually possible to record a sensitivity label in a V.2 segment, but I will leave that for further investigation, but there is guidance on how to label V.2 messages, basically. There is an emerging specification that has just been published as a draft. It has not been balloted, nor is it mature enough yet, but the privacy consent of FHIR is coming out of IG, and it does provide guidance of reporting and enforcing consent. It does address the integration with consent policy, and also, the maturity model is discussed to some extent. There is some level of advanced or intermediate. I see in chat that Hans is confirming that sensitivity labels can actually indeed be supported in a V.2 segment. Next slide, please.

So, to conclude, I want to mention a few key points. One is that to ensure that we do not leave any gateway open, and we cover all the possible ways that data can be shared, and at least the FHIR, V.2, and CDA are addressed if any requirement for security labeling and data segmentation is going to be enforced. I think it is very important and key to define a well-defined set of labels that are unambiguous and are understood by all parties and address use cases that are most pertinent to the community. I do not feel confident to lay out a set of labels myself, but I have a draft set in mind, and I think further feedback needs to be incorporated from all different stakeholders to determine that, but I think that would be in line with the alternative to basically take the current standards, but take kind of a modified approach to what exists in the current specification.

And then, I finally also want to emphasize again that recording sensitivity labels is something that is possible. There is extensive guidance on that, and there is sufficient guidance on recording sensitivity labels, but there is a risk of inconsistency in determining sensitivity labels because of the lack of guidance

on the common, underlying clinical concepts that would lead to the sensitivity labels. So, that is where I want to pause, and I apologize, I think I went over time. I will yield back to the chairs, and I would be happy to engage in the conversation.

Discussion (01:05:34)

Steven Eichner
Thank you so much for sharing. That was really useful and very informative. Hans?

Hans Buitendijk
There we go, unmute. Can you go back to the prior slide? Mohammad, I really appreciate the walkthrough that you have provided and the key conclusions that are there that I think we all should consider very carefully, particularly the elements in here that we can start to build something if we do focus. The way I am understanding this is that we have an opportunity to focus in some areas to align certain key vocabulary that therefore can be consistently interpreted by everybody as it is being shared, or how to consider that.

Looking at these four bullets, I completely agree that there are elements that need to be exchanged because they are essential to be maintained with the data as is, and internally, based on how your system operates, etc. you may have additional flags or other ways to easily get access to the data that you need to restrict or not, but you can always go back to the source core data based on which that is being done, and I think that is extremely important, and the guidance that we have elements in place, but making sure that it is consistently interpreted, that is fully aligned, there is the ability to do that, but we may not only have to look at FHIR, CDA, and V.2. The question is that in some areas, it is clear that the parties already need to exchange the data, it is fine, there are no restrictions to be communicated, but have we covered everything with these three? I would say a lot, but not necessarily everything.

The question that I have is on the third bullet, and that is the difference between sensitivity labels and, if you will, confidentiality labels if you look at the first one and those kinds of categories. I am curious, Mohammad. From that perspective, we have to be careful exchanging some of those because once they have been exchanged, the state may change. It is unclassified today, but it is confidential tomorrow. So, I am trying to get a little bit more perspective on how we help draw that line so that we can come to that small set of flags that we do want to exchange, whereas the other kind of flags are ones that you can use, and perhaps in combination with the patients' discussion and consent rules, it can be used to make it easier for a consumer to declare what they want to change or use them. I am going a little bit on the side here, but we need to do similar things with privacy rules established by jurisdictions because the combination needs to get in play. Can you clarify a little bit more where to draw that line on what to share and what not to share?

Mohammad Jafari
If I understand your comment correctly, you are saying that confidentiality labels are, in essence, a policy expression, and the policy may change after the data has been shared, right?

Hans Buitendijk
Correct.

Mohammad Jafari

Right. The confidentiality label on data that is being shared is reflective of the policies from the source's perspective at the moment that it was shared. So, if a patient designates something to be restricted or a jurisdictional policy actually leads to, for example, HIV-related data to be restricted, at the moment that is being shared, that is the expression of the source to say, "I consider this confidential," and if that changes in the future, I think that is a reflection of the changes in policy, and it may not necessarily apply to the recipient jurisdiction. I think there is some legal contention there, whether the policies of the source would prevail or the recipient's, so if the jurisdiction that is receiving the data is a different jurisdiction than the one that is sharing the data, which of the rules and policies should prevail?

I think the labels give us the tool to communicate those things, but the policy can still be applied by the general access control system on either side of that exchange. But I do want to concur with you that there is an inherent difference between policy tags, like confidentiality, obligations, and refrains, versus sensitivity labels that are inherently related to the content and the clinical content of a resource. I think a sensitivity label may change as a result of the change of the science of medicine, for example. That is the kind of radical change that would lead to us having to relabel sensitivity labels, but confidentiality labels are functions of policy, and the policy can change.

Hans Buitendijk
Thank you, that helps, and I think that, as you indicate, sensitivity labels change, hopefully very slowly, based on what is happening, and you probably have controls and ability to rederive them as needed based on new information that you have that everybody can apply consistently, because that is how we can define them in a much more rule-independent fashion, but the confidentiality labels and otherwise that are really policy tags can change, and the comment that I think we have to then look at as we progress is that it is at the time that the source classified it that way, and if we can recognize that, then we have opportunities to resolve that, where, later, it may change based on privacy or patient rule changes and can manage accordingly so that it is not going to yield conflicts and misinterpretations later, and I think those types of things on how to look at them in combination with how to apply the guidance are the areas where such implementation guidance profiling is still essential to best understand how we collectively share it. If we only provide sets of standards that are out there, then everybody has the opportunity to interpret it slightly differently or substantially differently. That is going to set us out on the wrong foot, so I think these are key elements to understand what is part of our first step and what can we grow in over time to make sure that can scale to the large variety of data that we need to manage.

Mohammad Jafari
Thanks, and I do want to note on that that the FHIR DS4P IG defines a set of extensions to actually convey the policy that was behind assigning the label or any related artifacts, like a policy document or a consent resource, so that would help communicate that I am considering this restricted or confidential based on this code that refers to, for example, 42 CFR Part 2, so we can reference the justification for assigning the labels, and also the identity of the labelers using those extensions, and that would help parse that out from the recipient's perspective.

Hans Buitendijk
Thank you.

Steven Lane

All right, great discussion. I am looking for other hands up. There we go, Sheryl. Thank you.

Sheryl Turney
Thank you for the opportunity to comment on this. Just a couple things. I know I brought some of these up yesterday, but I do not know how the certified health IT restrict data, but based on the way payers do it with sensitive services, it is quite complicated, and if we have to restrict data based on certain state obligations, based on some data that minors may have the right to restrict, etc., all of those things, at least for us, end up having to be done based on identifying CPT codes or some sort of coding system to earmark data that falls into those categories, which makes it very complicated.

I do not know enough about the tags that are being referenced within FHIR as to how those are or can be utilized when they are data that we are acquiring and then assimilating into our systems, so I think that is something where, at a minimum, again, we need patient education, they need to understand when they have restrictions, what that exactly means, that they are only able to apply that restriction to the physician that they are commenting on based on what everybody is saying in the comments that flow down is not something that would normally occur as a result of data restrictions.

I know for us, when a payer looks at data restriction, we look at any method that the patient has authorized to get that data. Sometimes there is a protective order, sometimes it is only impacting certain people or certain types of data, but normally, it has to be categorized into something that we can electronically organize and restrict, and so, I do not know that we have enough language or clarity here how that would really occur in a certified health IT system, so it does give me pause, and I also do feel as though we need to say something about the flowdown and the potential dangers that come with that, especially with all of the variances now between states and their positions on certain services that cannot be performed in some states, but can in others. I just think there is a lot of opportunity here for risk that somehow, we need to bring to the surface.

Steven Lane
We have Hans's hand back up.

Hans Buitendijk
I have a question for Mohammad, whether he can share any thoughts on another aspect of infrastructure. On the one hand, we have the need to understand the data as it is being shared, what it means, how it can be interpreted, and the rules can be applied to it consistently, a combination of sensitivity labels and confidentiality labels, if you will, to provide that, but one of the challenges as well, and particularly looking at it from a patient perspective, is that I am seeing multiple providers, data may be shared beyond that, and my rules change, and therefore, how do "chase down" that I changed my rule on one place, so how does it get recognized elsewhere?

On one end, you can say, "I am going to go to all the other places that I happen to know where the data likely is, and I need to change my rules there." On the other hand, if I do not have an easy way to manage that across all the places where the data actually might be and now need to be informed about the new rules, how do I do that? So, I am wondering what some of your thoughts are. On the one hand, we need these standards, we need to have that available as data are being shared, but how do we keep track of the changes in the rules?

Mohammad Jafari
That gets directly into the heart of the problem of interoperable consent and being able to basically express consent in a way that is completely computable and is also understandable in an interoperable way by different providers so that you do not have to go and change the rules at every single provider to be able to have consent utilities, to be able to have central places where a patient can choose to express their rules, and that can be applied to different providers from one place. I think having the consent resource used in a standardized way, and some of the work that was done in the LEAP Project and some of the work that has been done in profiling the consent resources, are the steps to make sure that the outcome of the rules is reported in a way that is standardized and is not dependent on the source of how the rules were authored. So, different consent management systems can help patients articulate the rules, and lead to consent resources that are standardized, and are computably understandable by different providers so that the rules can be mutually understood when they are expressed across the space by different providers.

Steven Lane
All right. Well, it is 10 minutes before the hour, and we are ready to go to public comment. That was a very active discussion.

Public Comment (01:19:48)

Michael Berry
Yes it is, thank you. As Steven noted, we are going to open up our meeting for verbal public comments. If you are on Zoom and would like to make a comment, please use the hand raise function located on the Zoom toolbar at the bottom of your screen. If you are on the phone only, press *9 to raise your hand, and once called upon, press *6 to mute and unmute your line. Let's pause just for a moment to see if any members of the public raise their hand. I am not seeing any hands raised, so I will turn it back to our cochairs.

Steven Lane
Ike, do you want to take us home?

Steven Eichner
We have a couple more minutes I think we can use for any subsequent discussion before we close out. I did want to give Hans a plus one on the idea of looking at the data flow and flowdowns, which I think gets made a little bit more complicated further if the patient does not have access to information about to whom their data was disclosed. I do not think it is within the scope of the rule per se, but it may be that the Task Force wants to include as part of summary content or perhaps a recommendation outside that providing continuous patient education about consent is an important idea, especially looking at where patient consent is not necessarily required for sharing information for things like PTO and what payment treatment operations and exactly what kinds of transactions are authorized in that space. That is just helping do a level-set between providers, patients, and technology vendors. Are there any other questions or comments in the last couple of minutes regarding data segmentation or the other material we have discussed today? Deven?

Deven McGraw
Thank you very much, Ike. My apologies, I messed up and did not originally accept my invite to be a panelist. That was user error on my part. One thing that does occur to me is that the state consent laws are very complicated, as I tried to chime in on the chat, and they feel like a use case that requires a more complete understanding of the scope of those laws to determine what kinds of technologies could be built in to help providers comply with them, but the HIPAA right to request a restriction, as Elisabeth from HHS pointed out, and then, also, maybe even the Part 2 data, because it is subject to federal law, does have some slowdown obligations and is currently in the process of being revised by HHS pursuant to some specific authorization from Congress, that that might be a use case that allows us to build in some capabilities for providers to leverage technology to help them comply with those obligations, and the right to restriction in particular is somewhat appealing because I believe that you really could let a patient know, "We are going to honor this prescription, but you need to understand that we may not necessarily be able to capture all of the inferential data, that it is not going to be applicable downstream, that it is just going to be about what we can control with respect to your disclosures of data."

You get to have that kind of conversation as part of the granting of that restriction because, as I think Sheryl was alluding to, except in the case of circumstances where the patient is paying out of pocket and requests the disclosure not be made to their health plan, it is completely voluntary on the part of entities to decide whether or not they want to grant them, but there may be an increasing desire to grant them in the context of very sensitive healthcare that now, as I do not have a better way to frame it, is subject to being weaponized against the patient or their medical provider in some jurisdictions. Thank you.

Steven Eichner
Thank you for that. I do want to encourage Task Force members to spend some time with the worksheets. We are getting to a point where we need to begin to really focus on the development of language that is in the form of a recommendation for the HITAC to submit to ONC. There has been some great discussion and great comments in the worksheets, but again, we need to focus and begin to transform it into things like "HITAC recommends that the language be changed," or "this consideration be made," or things in that space, so please do spend some time in the next week working on that space, so that will be a major focus for our work next week. I do want to thank our presenters. They did a fantastic job. I want to thank members of the public for attending, and thank you once again, Task Force members, for your time, energy, and contributions to a really interesting and useful discussion. Steven, do you have anything to add?

Steven Lane
We do still have four minutes, Ike. Let's not squander it, given how much is going on here. Sheryl, Dayo, Hans, Jim, and I have all put recommendations into the spreadsheet. I wonder, Ike, if you want to walk through these. Sheryl, is there something here that you said or that came up today that would translate into a specific recommendation? I think we lost Sheryl.

Sheryl Turney
No, I am not lost. Sorry, I just could not get off mute. Steven, I will go in and try to put something in in the form of a recommendation regarding patient restrictions and authorizations because I do think we need something in there, and I will work something up today.

Steven Lane
Wonderful. Hans, you have a couple recommendations in there, and you have had a lot of insight in the chat. I trust you will also have a chance to go in and update that.

Hans Buitendijk
I certainly will.

Steven Lane
Wonderful. I took a stab before today's meeting at trying to get very specific in recommendations, suggesting some specific inclusions and limitations, so I will be veery interested in other workgroup members' responses to those very specific recommendations, or perhaps, Hans or others, if you want to incorporate something similar, feel free to redline mine if you want to make specific changes. Jim, I think you have raised some really important points today about feasibility and what we can reasonably accomplish in a single turning of this wheel. Do you want to comment on that? What do you see personally as the sweet spot?

Of course, we need to give very specific recommendations back to ONC, not general observations, so do you have a sense of how we can do that? Jim, you are on mute. Jim might have been pulled away, but again, hopefully, we will all have that chance. Good question, Hans. So, Group 1 and Group 2 are really supposed to address different issues, Group 2 the specific recommendations that were entered in Group 1 and more what else ONC should be doing in this domain in future rulemaking, or at least that was my impression, so I think we should try to separate our comments in that way, unless ONC has a better suggestion.

Hans Buitendijk
Okeydoke.

Steven Lane
Great. Mark, thank you for your comment. Ensuring that individuals understand what is occurring is certainly critical. All right, well, Ike, do you want to send us off?

Steven Eichner
Sure. Now we really are at the top of the hour, and it is time to close us out. Again, thank you for all parties' participation and contributions. Have a great week.

Hans Buitendijk
Thank you.

Adjourn (01:29:13)