National Committee on Vital and Health Statistics

Transcript

March 25, 2020, 8:30 a.m. – 3:00 p.m. ET

VIRTUAL

SPEAKERS

NCVHS Members		
Name	**Organization**	**Role**
William W. Stead	Vanderbilt University	Chair
Sharon Arnold	DHHS	Executive Staff Director
Rebecca Hines	NCHS	Executive Secretary
Alexandra Goss	Imprado/ DynaVet Solutions	Member
Debra Strickland	Conduent	Member
Denise Chrysler	University of Michigan School of Public Health	Member
Denise E. Love	Individual	Member
Frank Pasquale	University of Maryland Carey School of Law	Member
Jacki Monson	Sutter Health	Member
James J. Cimino	University of Alabama at Birmingham	Member
Lewellyn J. Cornelius	University of Georgia, Athens	Member
Margaret A. Skurka	Indiana University Northwest and Principal, MAS, Inc	Member
Melissa M. Goldstein	The George Washington University	Member
Nicholas L. Coussoule	BlueCross BlueShield of Tennessee	Member
Richard W. Landen	Individual	Member
Vickie M. Mays	UCLA	Member
NCVHS Staff		
Name	**Organization**	**Role**
Susan Queen	NCHS	Staff
Maya Bernstein	ASPE/OSDP	Staff
Lorraine Doo	CMS	Staff
Rachel Seeger	HHS Office for Civil Rights	Staff
Amy Chapper	CMS	Staff
Natalie Gonzales	OADS	Staff

Geanelle Herring	CMS	Staff
Kate Brett	NCHS	Staff
Marietta Squire	NCHS	Staff
Donna Pickett	NCHS	Staff
Consultants/SMEs/Others		
Name	**Organization**	**Role**
Vivian Auld	NIH	
Tom Mason	HHS	ONC
Lauren Richie	HHS	ONC
Presenters		
Name	**Organization**	**Role**
Naomi Lefkovitz	NIST	Senior Privacy Policy Advisor
Edward H. You	HHS/Office of National Security	Liaison Officer
Chris Muir	ONC	Director, Standards Division
Stephen Konya	ONC	Senior Innovation Strategist

Call to Order/Roll Call

Rebecca Hines: Good morning everybody. Welcome to the National Committee on Vital and Health Statistics, the advisory body to the HHS secretary. This is day two of our Spring Meeting. Welcome back to those of you who were with us yesterday, members of the public, and again, a warm welcome to our members. Thank you very much for your service. Yesterday was a fabulous meeting. I thought it went very well for our first virtual Zoom committee meeting.

I wanted to pause before taking roll call and just say this morning I read this article in the Times by a deputy editor. She wrote an article called "What I Learned When My Husband Got Sick With Coronavirus". It really brought it home that while we are sitting here meeting, she said it is very surreal to be in this world of panic and constantly deciding whether or not her husband is ready for the hospital, while we are carrying on. It is just something to bear in mind during this truly unprecedented time.

She is a beautiful writer. Very compelling. Anyway, I just want to point you to that piece.

Now on with our business. We are fortunate that we can all continue, that we are all well. My name is Rebecca Hines, I am the executive secretary and designated federal officer. Let us go to our chair to begin. Bill Stead.

Bill Stead: I am Bill Stead, Vanderbilt University Medical Center, Chair of the Full Committee, no conflicts.

Rebecca Hines: Denise Chrysler.

Denise Chrysler: I am Denise Chrysler. I am on the Full Committee, on the Privacy, Confidentiality and Security Subcommittee, and I have no conflicts.

Rebecca Hines: Lee Cornelius.

Lee Cornelius: I am Lee Cornelius. I am at the University of Georgia. On the Full Committee, Population Health Subcommittee, and I have no conflicts.

Rebecca Hines: Nick Coussoule.

Nick Coussoule: Nick Coussoule, Blue Cross/Blue Shield of Tennessee, member of the Full Committee, Standards Subcommittee, Privacy, Security and Confidentiality Subcommittee, and I have no conflicts.

Rebecca Hines: Melissa Goldstein.

Melissa Goldstein: Good morning. I am Melissa Goldstein. I am a professor at George Washington University. I am on the Full Committee and the Privacy, Confidentiality and Security Committee, and I have no conflicts.

Rebecca Hines: Alix Goss.

Alix Goss: Good morning. I am Alix Goss with Imprado, the consulting division of DynaVet Solutions. I am a member of the Full Committee, a member of the Executive Subcommittee, Co-chair of the Standards Subcommittee, and Review Committee. I have no conflicts but did just want to note my involvement

with the FHIR at Scale Task Force. We will be having a presentation on that later today. I am not only a Tiger Team co-lead for Directory Version and Scale Architecture, I am also on the Steering Committee.

Rebecca Hines: Thank you, Alix. Rich Landen.

Rich Landen: Good morning, Rich Landen, Florida, member, Full Committee, member, Executive Subcommittee, Co-Chair Standards Subcommittee, no conflicts.

Rebecca Hines: Denise Love.

Denise Love: Denise Love, consultant to National Association of Health Data organizations. Member of the Full Committee, member of the Standards Subcommittee, no conflicts.

Rebecca Hines: Vickie Mays.

Vickie Mays: Vickie Mays, University of California, Los Angeles. I am a member of the Full Committee, Population Health, Privacy and the Review Committee on Standards, and I have no conflicts.

Rebecca Hines: Jacki Monson.

Jacki Monson: Good morning. Jacki Monson, Sutter health, member of the Full Committee, member of the Subcommittee on Privacy, Security and Confidentiality, no conflicts.

Rebecca Hines: Frank Pasquale.

Frank Pasquale: Frank Pasquale. Member of the Full Committee and Co-Chair of the Subcommittee on Privacy, Confidentiality and Security, no conflicts.

Rebecca Hines: Margaret Skurka.

Margaret Skurka: Margaret Skurka. I am a member of the Full Committee. I am a member of the Standards Subcommittee and I have no conflicts.

Rebecca Hines: Debra Strickland.

Debra Strickland: Hi, I am Debra Strickland, Conduent. I am a member of the Full Committee, member of the Standards Subcommittee and I have no conflicts.

Rebecca Hines: And the executive staff director Sharon Arnold is not with us today, with the Assistant Secretary for Planning and Evaluations Office. We have some other lead staff, Rachel Seeger. Do you want to say good morning?

Rachel Seeger: Good morning. Rachel Seeger, HHS Office for Civil Rights. Thank you.

Rebecca Hines: and Rachel is our lead staff for the Subcommittee on Privacy, Confidentiality and Security. And on Standards, Lorraine.

Lorraine Doo: Good morning. This is Lorraine Doo, currently with the Health Informatics Office at CMS. Lead staff to Standards Subcommittee.

Rebecca Hines: Very good. I believe that is roll call and we have a quorum. I will turn it back over to you, Bill.

Welcome Remarks/Agenda Review

Bill Stead: Thank you Rebecca. Let me just one second, thank Rebecca for her context-setting originally at the start of the morning. We are really living in unusual times and I am grateful that people are making the time to do this work while we try to stay well, take care of our families, and deal with the crisis in the health system.

Just briefly review the agenda, the bulk of the morning is going to be focused on – actually the whole morning, is going to be focused on the work of the Privacy, Security, Confidentiality Subcommittee. We are going to start with a overview of the NIST Privacy Framework. Then an update on Safeguarding the Bioeconomy. Then the working block with the Subcommittee on Privacy, Confidentiality and Security on their options and alternatives for their workplan going forward.

Then after lunch we will have an update on the FHIR Scale Task Force, that Alix mentioned. We will close by walking through our workplan and making any edits we want to make based on what we have learned over the course of these two days.

So that is the plan. Did I miss anything Rebecca?

Rebecca Hines: That sounds right.

Bill Stead: Any questions? Seeing no hands comes. It is my privilege to introduce Naomi Lefkovitz. Thank you for being up to help us this morning. She is the Senior Privacy Policy Advisor for the National Institute of Standards and Technology and she is going to provide an overview of the NIST Privacy Framework. I have at least, found that Framework to be extraordinarily helpful, particularly the way that it shows the intersection with the Cybersecurity Framework and how they work together.

Welcome, Naomi.

NIST Privacy Framework

Naomi Lefkovitz: Thank you and thank you for having me. So let us get started. I am very happy to talk about the framework, just to give you a little bit of background about the development so that you understand sort of the posture that we developed it under. It sounds like you are also – that people are hopefully generally with the Cybersecurity Framework.

In about, I think like the summer of 2018, we were getting some inquiries from industry and the Administration. Given the landscape of privacy and the new regulations coming out both in GDPR and California and so forth, as well as some various major privacy incidents in the news, there were some questions about given what NIST did with the Cybersecurity Framework, whether we could do something similar for privacy. So that really launched us on the development process.

Since it was going to be a voluntary tool and NIST, as everyone probably knows, is non-regulatory, we thought that at the very least the Cybersecurity Framework showed us a path or model for a development process that was very collaborative with stakeholders, very open and transparent with the hopes that when you run a process like that then you actually are meeting the needs of the stakeholders

in terms of developing a tool that they will want to use at the end of that process. So that was our initial goal, to at least model the process after the Cybersecurity Framework but, similarly, to go into that with a very open mind about what the product would be at the end.

Like the Cybersecurity Framework, we had a request for information and various public workshops and webinars, and over the past year -- mostly in 2019 -- we went through various draft iterations, and the result is Version 1.0 which we released January 16th. I just wanted to give you a little sense of that process so you could understand how we got to this voluntary tool.

This being a voluntary tool, the value proposition is very important. Why would anybody pick this up? So this is the message that we honed with stakeholders over the year and is in the Executive Summary.

First and foremost, we really see this as a tool to help organizations manage privacy risk, and so it is really about building customer trust through supporting organizations to be able to engage in ethical decision-making to optimize beneficial uses of data while minimizing adverse consequences to people or even society as a whole.

That said, we certainly understand that privacy exists increasingly in a very regulated environment, and so we see the framework as being able to help organizations fulfill their current compliance obligations. By that we don't mean that just complying with the Privacy Framework is going to equal compliance with any particular law or regulation you might be subject to, but rather, we see the framework as sort of providing the building blocks in policies and the capabilities that you might need to demonstrate how you're fulfilling particular legal obligations.

That actually leads nicely to the third point about how we see the framework supporting communication, and that communication is both inside the organization, across different parts of the organization, as well as with external organizations whether those be vendors or other business associates or whatever organizations you might be engaged with, as well as even potentially regulators -- getting back to that point of saying, hey, we can show you the kinds of measures that we are taking to help meet specific legal obligations.

Those are the main key points that we work on with stakeholders to demonstrate the value.

This discussion about cybersecurity and privacy risk was a significant part of the development process. When we put out our first request for information, we asked what are organizations' privacy risk management practices? How do you define privacy risk? I think it was very clear from the answers that we got back -- I think the only consistent answer was there wasn't any consistency, which is very different from the cybersecurity space. If you ask anybody who works in cybersecurity how do they define risk they are going to give you some very close variation of what is the likelihood that a threat will exploit a vulnerability and the impact if that occurs.

We don't have that consistency in privacy. There is certainly a strong understanding of data security and how that relates to privacy in terms of individuals' personal information or health information, but we don't really have a good understanding or sort of a uniform way to talk about privacy risk that extends beyond cybersecurity risk. That is, certainly, cybersecurity is important for protecting privacy but it doesn't do the entire job.

To give you one example of what we mean by that, we sometimes use this example in the smart grid where there are communities that were objecting to smart meters not so much because they thought

the information couldn't be kept secure but because the information that was being collected by the smart meters was so granular that inferences could be made about people's behavior inside their homes. That is not really an issue of confidentiality in the sense that there was unauthorized access but, rather, people's discomfort with feeling like there might be surveillance inside their homes.

And so we came to look at this as sort of this Venn diagram, describing the right side of the Venn diagram as thinking about how organizations may be doing data processing, and by data processing we mean this complete data lifecycle, so, everything from collection through disposal, and that they are doing that data processing really to achieve mission or business objectives. So the smart meter had a positive benefit in terms of helping to manage energy more efficiently, which is good for society.

But, at the same time, individuals can experience what we sort of termed as problems arising from that data processing, and those problems can range from feeling embarrassed about something that got revealed or even discrimination or loss of self-determination or feeling like they might being surveilled and then change their behavior inside their homes. And so we think of problems as sort of a meta term like threats in the cybersecurity model. That is, you can put in any value that is relevant.

And that bring us to enabling us to develop a model for analyzing privacy risk in systems or products or services where we can now say what is the likelihood that individuals will experience some kind of problem from data processing, from some sort of data operation, and the impact if that should occur.

I will leave time for questions but if there is anything critical, feel free to jump in with a question. But with that background, let's go to the next slide.

This led to another big conversation with stakeholders which is, okay, if we can understand privacy risk as this likelihood and impact of problems arising from data processing, how does that relate to organizational risk. We really see the Privacy Framework as being a tool for enterprise risk management, and we see that by recognizing that individuals are going to experience the direct impact of problems. They are the ones who are going to be embarrassed or feel the effects of discrimination or economic loss.

But organizations almost feel sort of a resulting impact; that is, they sort of manifest the impact through different aspects like customer abandonment -- when customers lose trust in products and services they either are slow to adopt them or they abandon them -- or non-compliance costs or harm to reputation or internal culture. Think of the employee walkouts that have been in the news.

And these types of impacts on organizations -- they can come from a variety of reasons or sources, and organizations have been managing them traditionally at that enterprise level. So our thought is that if we can make privacy risk more visible with the experienced individuals, more visible to the organization and help them understand that those impacts, through the kinds of impacts that they traditionally manage, perhaps we can bring privacy risk into greater parity with other enterprise risks and, ultimately, have a more appropriate allocation of budget and resources to strengthen privacy programs.

As I mentioned, when we were exploring privacy risk management practices with organizations it was not a surprise to us, but it was made very clear that privacy risk management is not as well understood as cybersecurity risk management. As a result, although we were very clear the Privacy Framework is not the be-all and end-all of guidance -- in fact, it's an area that needs a lot more work in order to get to the same level of maturity as cybersecurity -- we did think that it was important to put a little more information and a little bit more guidance into the Privacy Framework than you would see in the

Cybersecurity Framework where people were coming to it with just a more uniform, broader understanding.

And so we have a section speaking to the role of privacy risk assessment, which is a very important sort of sub-process in the overall practice of privacy risk management. The way we approach this is by trying to address some key questions that we have gotten, frankly, over the years, because the work that we are actually leveraging, since we didn't find anything coming from stakeholders, is actually the work that we have been doing in the privacy engineering program for the last several years.

The questions that we have gotten over the years almost come at two ends of the spectrum. One end of the spectrum is, hey, I think what I am doing with data is really beneficial. It's almost like how do I make sure that privacy doesn't get in the way of that? And the other question comes from almost the other end of the spectrum which is, how do you know when you shouldn't be doing some kind of data processing, essentially where the risks outweigh the benefits?

Both of those questions really get answered by this process of privacy risk assessment. Once you have identified and assessed your private risk, then you are able to think through what the appropriate response is, and responses traditionally in risk management sort of fall into four general categories. One is mitigation where you can't get your risk level to zero but you can put in reasonable measures or safeguards that will at least mitigate your risk down to an acceptable level.

Another one is avoidance, and that is essentially where you are saying, okay, this risk is too great and we are not going to take it. So that might be an instance where you might decide that the data processing is too risky and the harms or potential problems for individuals outweigh the benefits and you are going to avoid that risk by not doing the data processing or stopping the data processing.

And then there is acceptance. Here, the benefits are high and the risk may be minimal and you might decide that you can accept it and the cost; therefore, it is not really worth the cost invested in trying to mitigate.

And the other one is sort of transfer or sharing. That is traditionally among organizations where transferring or sharing risk is done through contracts, and we actually see privacy notices and consent options as a means of sharing risk with individuals.

We really want to impress upon organizations how important privacy risk assessment is to actually building that customer trust that I referenced in the beginning, and really to help figure out how do I go through that process of ethical decision-making about optimizing benefits of data while minimizing adverse consequences for individuals.

As I said, although we can't make this document everything to everyone in terms of providing every aspect of guidance on privacy risk management, we and hopefully the community will continue to develop a body of work that will be equivalent to cybersecurity.

But we did want to give just a little bit more information, so we developed this Appendix D which has the key privacy risk management practices. For the sake of time I am not going to go through every one of these, but you can see that we talk through the kinds of resources that could be helpful in terms of data maps and enterprise risk management strategies and artifacts that help you understand the data processing in your systems.

And then thinking about how do you determine the kinds of privacy capabilities that you want in your products and services, which allows you then to start thinking about how you define the specific privacy requirements. And some of those requirements are going to come from your laws or regulations that you are subject to or your internal policies, but some of them will also come from conducting your privacy risk assessment so you can define how do I want this system to operate in terms of achieving the kinds of privacy capabilities that I want in that system.

And then, ultimately, that allows you to select and then implement and assess controls, which really creates that traceability back to saying yes, I am actually meeting the privacy requirements that I had set for this system.

And then, of course, this is an iterative process where you need to monitor the environment for changing privacy risks, whether that's because you are using a new technology or new laws have come into play or you have changed your business process in some way. Hopefully, there is a good wealth of information at least to get people started on thinking about privacy risk management.

One other thing I would say about that is we really tried to make some connections to other NIST guidance, for example, Special Publication 837, the Risk Management Framework, as well as a privacy risk assessment methodology that we developed to help actually walk through the process of privacy risk assessment.

With that background and some of those concepts, we can now talk about the actual structure of the framework. This should actually look pretty familiar to you. We heard very clearly from stakeholders early on in the process that they wanted to see the Privacy Framework aligned with the Cybersecurity Framework, and so we took the three components of the Cybersecurity Framework, the core, the profiles and implementation tiers and essentially adapted those to the privacy data processing, sort of the right side of the Venn diagram.

Like the Cybersecurity Framework, the core is really about providing an increasingly granular set of activities and outcomes that enable an organizational dialogue, in this case about managing privacy risk.

The profiles really drive the risk-based approach of the framework. That is, the activities and the outcomes in the core are not intended to be a checklist, and the profiles are a way to prioritize which activities and outcomes are most important to the organization in terms of managing the privacy risk. And then the implementation tiers are a generalized set of benchmarks that help organizations think through whether they actually have sufficient processes and resources in place to manage that privacy risk and hopefully achieve their target profile.

We will go a little more depth into these components. Again, if you are familiar with the Cybersecurity Framework this should look very familiar. The way we get that increasingly granular approach is to move from high-level functions down to categories and then to subcategories. What we found with the Cybersecurity Framework was that the high-level functions were very helpful for communicating with the C-suite or the Board in terms of they weren't cybersecurity professionals generally; you are not going to have deep conversations about encryption with them but sort of these simple, intuitive terms that help them to very quickly understand how you are managing cybersecurity risk. And so we wanted to see if we could accomplish that for privacy as well.

You might see some overlap -- for example, identify exists also in the Cybersecurity Framework, and I think that makes sense because those are generally high-level, organizational-level activities. So, in adapting them to privacy, the process itself is not that different.

But I think what is a little bit different is what we heard from stakeholders that the government processes that were embedded or are still embedded in Identify in the Cybersecurity Framework were so important to privacy that they needed to be elevated into their own function. So, if you look at Govern -- I don't know if you provided the slides in advance or you're posting them, but we did provide at the end some slides on the core, and if you look at that I think you will see that, again, the content for the most part is very similar to the Cybersecurity Framework. We just basically split Identify into two categories.

One place that Identify really differs from the Cybersecurity Framework is that rather than focusing on asset management, we created a Do category called Inventory and Mapping because there is a little bit about data flows in the Cybersecurity Framework, but we felt, along with stakeholders, that really understanding the data processing and mapping that in your system or your products or services is so critical to managing privacy risk that it really needed its own dedicated category.

As you work your way down through the categories and the subcategories, you get increasingly granular and move down the stack in the organization. A lot of the subcategories are really where you develop policies that you need as well as talking to engineering about an IT, about the capabilities that you might need to really manage privacy risk and meet your privacy requirements, whether those are coming from your legal or regulatory environment or your internal policies.

One example I can give is in the Control function, which is really about managing the data processing. Perhaps under Govern, for example, you identified a legal requirement to take data deletion requests from individuals, and so at Govern you are also going to presumably set some kind of policy about what data and how you are going to take those requests.

In Control, we have some subcategories around enabling access to data for deletion, and that is really about focusing on the capability. For example, if you can't go into your system and find and extract data, then your ability to actually meet your policy and ultimately that legal requirement will just simply be aspirational.

So that is how we see these building blocks fitting together with both the policies and the actual capabilities that you need in your systems.

This is what Bill was mentioning. We had a lot of discussion and lot of questions about how does this align with the Cybersecurity Framework, then? How do organizations use these two frameworks together? The conversation over the year is there are almost like two camps. One camp felt that there really shouldn't be an overlap between the two, and the other camp felt that there should be a lot of overlap. And the reasons seem to sort of fall out along whether an organization already had strong collaboration between their privacy and security teams or how robust or mature the privacy program was.

And so, even though at NIST philosophically we very much support strong collaboration between privacy and cybersecurity teams, we felt that we needed to meet organizations where they are today, and so we wanted to show the flexibility of how you could use the two frameworks together. We thought

essentially take that Venn diagram I showed you earlier and overlay the functions so you can see where were the primary functions that help manage different aspects of cybersecurity and privacy risk.

If you're thinking about the data processing aspect of privacy risk, then Identify-P, Govern-P, Control-P, Communicate-P, to indicate that they are from the Privacy Framework, those are the primary functions. But if you are in that overlap space, sort of data security around, say, health information or personal information, then you can add Protect-P, which is highly overlapping with the Protect in the Cybersecurity Framework but it has a little bit more the lens of viewing it from the privacy aspect. So it can really help organizations that might not have very mature programs or need more help communicating with their cybersecurity team about aspects of Protect that are privacy-related.

At the same time, because Detect, Respond and Recover are so cybersecurity incident-focused, we just didn't feel that in sort of meeting that middle ground that replicating them in the Privacy Framework was as critical as Protect, and so organizations can just pick those up and use them and apply them to privacy breaches.

And moving over to the left, an organization might already be using the Cybersecurity Framework, and as a result there might already be strong collaboration, they might already be using the framework to address these cybersecurity-related privacy events, and they just need to pick up the other four functions to address the data processing side. So, hopefully, that shows some of the flexibility in the ways that you can use the two frameworks together.

We have already heard from some organizations that have taken that additive approach because they were already using the Cybersecurity Framework and they actually found it relatively easy to analyze that gap space and add in additional controls.

We also recognize that there still is some complexity here, where flexibility can bring complexity, and so it's certainly going to be an ongoing conversation that we are having internally as well as with stakeholders about how do we continue to simplify and better align our approaches to these frameworks.

As I mentioned, Profile is really again the same concept from the Cybersecurity Framework. The core is not a checklist; you can look through it and use it as a dialogue or conversation starter within your organization about what activities and outcomes are we doing today, and that would result into your current profile.

But as you consider your organizational goals, your role in the data processing ecosystem or industry sector, one of the things is we really tried to make this agnostic to any particular law or regulation, so you won't see terms like data controller or data processor in the framework. But we recognize that, at least if you are subject to things like GDPR or California, those terms are sort of codified rules and can have an impact on the kinds of requirements you need to be cognizant of.

And so understanding your role as well as your legal regulatory requirements, your risk management priorities and, of course, the privacy needs of individuals, taking those all together can help you identify where you -- moving from your current profile to your target profile -- where you may have gaps, and that would allow you to develop an action plan and have that conversation inside the organization about the kinds of resources you might need to achieve that target profile. That, in fact, allows you to have a deeper conversation about the types of resources or processes you might need to build to achieve that target profile.

We see the implementation tiers as really helping organizations to walk through these questions. Now that I understand my privacy risks, do I have sufficient resources and processes in place to manage these risks? So the tiers are set at one through four, with four different elements.

One thing we did change from the Cybersecurity Framework is we added an element for workforce to help organizations think through how diversified does my privacy workforce need to be, and do I have the right level of training for my workforce.

The philosophy on implementation is not that everybody necessarily has to get to a four, but, thinking about the privacy risks you need to manage, are you at the right tier. For example, taking workforce, at two we have described workforce as you have somebody who understands something about privacy risk but perhaps wears multiple hats in the organization, and that might be fine for the kinds of privacy risks you need to manage. On the other hand, it might not, and maybe you need to get to a two or three or four with a four in workforce being a highly diversified workforce, you know, where you're going to have a chief privacy officer down to privacy engineers and various roles in between. So that is just an example of how you can use the tiers.

For the sake of time I am not going to go into this slide in depth, but the main point of the slide is to show that there are lots of ways to use the Privacy Framework, and as I mentioned earlier, we don't see -- in fact we don't even really talk about -- compliance with the Privacy Framework because there are so many ways to use it and it's difficult to say what compliance would mean. But that said, we tried to provide information about how you can use this to establish or improve a privacy program, and we have actually provided some hypothetical use cases on our website.

We talked about this data processing ecosystem. In the Cybersecurity Framework you would see that as the supply chain, but it was interesting. For stakeholders, that term didn't really resonate with stakeholders through the process, so we came up with this term, the data processing ecosystem, so that you can think about not only how do you manage privacy risk from your internal standpoint but what are you doing and how is that impacting other organizations' ability to manage privacy risk.

And so we have had conversations in the IOT, Internet of Things, space with manufacturers who said, well, I just make the device; how others use it and what they do with the data, that happens in their environment. We were like, well, that is true, but at the same time the kinds of capabilities that you build in or don't build in regarding privacy into your devices can have a real impact on other organizations' ability to manage privacy risk in their environments. So that is sort of the concept that we are trying to convey when we think about how does the Privacy Framework help with the overall data processing ecosystem that every organization should be thinking about privacy risk from their standpoint.

The one other piece that I want to mention, if you notice the informative references and if you are very familiar with the Cybersecurity Framework you might be wondering what happened to the informative references. We made a decision not to embed any informative references into the Privacy Framework because some of the lessons learned with the Cybersecurity Framework were that those references can get out of sync over time. As they get updated they can get out of sync with the frameworks.

What we did instead is we have created on our website this resource repository where we have put relevant NIST guidance and tools and some crosswalks with the Cybersecurity Framework. Our goal is to have the community also contribute to this repository to create more crosswalks, common profiles, more guidance and tools that can help organizations achieve different subcategories. We are working

with our colleagues at OCR to hopefully produce a crosswalk between the Privacy Framework and the HIPAA privacy rule, so stay tuned on that.

We hope that will be helpful to organizations to think about, if I am trying to meet the privacy rule, what are some of the basic subcategories that I should be focused on and prioritizing, and provide that as a floor, not that an organization couldn't add to that for their profile but at least it can help organizations think about what a base profile might look like.

I will just say a few quick words about next steps. This dog actually has a happy home, but the Privacy Framework would still like to be adopted. We have had organizations that have already stepped up and said that they are publicly using the framework or they have given us quotes that we can put on our website to show leadership on privacy. We found that was really important with the Cybersecurity Framework where organizations were willing to step up and other organizations saw that and it helped to bring them on as well.

But if that is not something an organization might want to do, we certainly look for any kind of implementation feedback so that over time we will revise the Privacy Framework. We consider it a living document. We want to make sure that it continues to evolve to be useful and meet the needs of stakeholders.

Lastly, as I said, contributing resources to the repository is another way to support the framework.

Borrowing another concept from the Cybersecurity Framework, we did this companion roadmap to highlight some areas where there continue to be challenges, and it is sort of a guide to NIST areas to do additional work and additional collaboration with the community. So, as I mentioned, privacy risk assessment us an area where more work needs to be done, more guidance needs to be developed but, also, mechanisms to provide confidence, whether those be assessment criteria for controls or additional certifications or criteria for building on certifications.

Also, emerging technologies. I mentioned IOT, but AI, of course, the impacts and how do we develop the framework to better help address these emerging technologies -- de-identification techniques as well as, given these emerging technologies, how that is going to change re-identification risks.

Inventory and mapping I mentioned. Our ability to develop more technical standards, for example, in differential privacy to help with better de-identification.

Privacy workforce continues to come up over and over again with organizations, so we are looking at can we work with our already existing, nice framework and perhaps build out or add on to that for privacy. And then our continuing work internationally and how do we better align and address some of the regulatory aspects and impacts coming internationally.

So those are some of the areas. We certainly have our work cut out for us but we look forward to engaging with you and other stakeholders to address these areas.

As I said, there are other slides in here to show the core so we are happy to share these slides and happy to take any questions.

Rebecca Hines: Naomi, thank you so much. That was really helpful to get some of the background underlying the framework. We did email out the framework to people last week so hopefully at least the

members of the Subcommittee on Privacy, Confidentiality and Security had a chance to look at that in advance. I will go ahead and send these slides out to the members.

Let's open it up. I see some hands. Denise Love, do you want to start it off?

Denise Love: Yes, I am a little intimidated with all the privacy folks online, but I will be a little provocative here. Thank you for the presentation.

I am just sitting here listening to this wonderful framework, but how does it apply to public health? Just in my travels over the last decades it seems like we are developing or have several different ecosystems and not one, and I am not sure how public health fits into this because they are not really querying, they are more required to push information, and they have different missions sometimes than the private sector. How does it all fit in, or does it?

Naomi Lefkovitz: When you say a different mission, we certainly have local governments as well as federal agencies who have already started to adopt this. Certainly you have missions and you're developing agencies, and local governments are developing services and products that use data and I think even in today's environment with COVID19 there are all kinds of privacy discussions going on about not only the collection of data but even the tracking of people to manage very beneficial needs to contain the virus. But already there are conversations going on about how do we do that in light of the kinds of values we have as a society.

Denise Love: I appreciate that. It's just that the technical framework is great, but my problems have always been human factors, getting people to trust each other. One of the areas in public health that I have struggled with, and maybe the privacy folks can help, is even with all the technology and things that we have at our disposal, redaction is one example where it is poorly applied or unevenly applied for sensitive information for public health. That is just one example.

But I just wanted to raise this issue that I am not sure how the TEFCA fits in right now with public health. But that's more of an open question maybe for the privacy folks.

Rebecca Hines: Rachel, I see you had a comment. Feel free to share.

Rachel Seeger: Sure. Denise, public health authorities are covered entities under the HIPAA privacy rule, so, many state, local and county health departments play in our space, and outside of the HIPAA privacy rule NIST is offering a privacy framework that in many ways provides technical assistance in approaching privacy through a risk assessment.

It is just really helpful, and we hope that we can help facilitate getting this framework out to folks so they are more aware of it. As Naomi said, the timing can't be more perfect because we are being inundated right now with questions from public health authorities about HIPAA-permitted uses and disclosures during this national public health emergency.

Denise Love: I bet you are. Thank you. I will look forward to the discussion.

Rebecca Hines: Frank, I see your hand up.

Frank Pasquale: Yes, and thank you for a very comprehensive framework.

One thing I was wondering in terms of thinking about how -- you mentioned breaking this down for the C-suite or breaking it down for people who are not privacy experts. I do a lot of work in that area in terms of thinking about how to naturalize or how to make more natural and more accessible very complex ideas about data management and control.

I was wondering, Naomi, what your opinion would be of this breakdown, which is could we explain the key aspects of provenance orientation or determination and control by saying that any entity should know where its data is coming from and should record where its data is going to. Would that be sort of a basic ideal upon which one could build larger duties for data?

Naomi Lefkovitz: Yes, absolutely. The only thing I would add to that is sort of the middle piece of what you are doing with data when it's not coming or going, both from analytics and inferences as well as storage, from the data security standpoint.

Frank Pasquale: Absolutely. Thank you.

Rebecca Hines: Melissa.

Melissa Goldstein: Good morning, Naomi. Thanks very much for the presentation. It was really helpful, and I think the slides are actually very helpful, too, in explaining what some people might think of as a very complex structure.

This is back to Denise's question and Rachel's response about public health. My experience in teaching public health law and being a public health law scholar has been that privacy issues have always been present in public health activities, especially in pandemics and in situations where we have emergency responses.

My question for Naomi is do you know of any public health authorities or public health departments that have adopted the framework so far? Because I think the concept of all of these entities conducting a risk assessment is so useful because some public health authorities are not necessarily HIPAA-covered entities because they don't provide services.

So, if you are a public health authority or department that doesn't actually provide services or meet the definition of a HIPAA-covered entity, it might still be very important for you to conduct a risk assessment as a first step. I'm wondering if you know any information about that so far.

Naomi Lefkovitz: So far, we have talked to county-level organizations. Almost invariably, when we talk to them -- you know, they have a program that's broader than just health, but invariably they always talk about their health department as one of their use cases. We are certainly, as I mentioned, working with OCR in terms of developing a crosswalk, but beyond that I haven't heard directly from public health departments yet, but we hope by doing these kinds of briefings that we can spread that word and have you all be able to spread that word.

And our contact info is here. We very much want to hear from anyone who has questions about implementation. I think we have several calls a week talking to either companies or public sector agencies about how to do implementation.

Melissa Goldstein: Thank you. I think this has great promise for the public health world.

Nick Coussoule: Naomi, thanks again for the presentation, really helpful. You mentioned during the presentation and then just a minute ago working with OCR to develop a crosswalk. Can you tell me how that is progressing or if there is any kind of timeframe that you're looking at, or what else might be happening there?

Naomi Lefkovitz: I think we have had some back-and-forth, so I think we're finalizing the details. I know they are a little busy, so I don't want to put them on the spot in terms of a timeline that we have anticipated, but it's a little bit disrupted. But we certainly hope in the next months that we will get that finalized.

I will say it was a very interesting process. This is the inventory and mapping category, and we tell that it wasn't necessarily any sort of one-to-one relationship between -- You know, the HIPAA privacy rule didn't necessarily say something about inventorying your systems and products and services or any of these other activities. But what we did was we have actually mapped that to some of the disclosure requirements and the notice requirements, because if you haven't actually done this and you haven't actually inventoried the purposes for your data actions then how do you know whether you can disclose something or not, whether you are in an accepted disclosure or what to put into your privacy notice.

So we found that, and I think OCR colleagues found it, very interesting that we could use the framework to demonstrate what are some of the underlying activities that you will need to do to actually be able to properly achieve your requirements from the privacy rule.

Rebecca Hines: Nick, anymore follow-up?

Nick Coussoule: No. I think that is very helpful. We are quite interested in that here. We have done a little bit of that ourselves just operationally as we try to mature our own organization, so I was just curious as to how that was proceeding. Thank you. I appreciate it.

Rebecca Hines: Rich, you have your hand up?

Rich Landen: Thank you, Naomi. Very, very good presentation. I am impressed with the thought that goes into it and particularly with the alignment with the Security Framework.

My impression, though, is that in order to really take advantage of this framework or tool you're talking about entities that are large enough that have a fairly substantive corporate staff with privacy professionals we have employed or are under contract with dedicated resources there. It's an observation and I'm struggling with where to take it.

But thinking about the healthcare delivery system in the country, I am not quite sure I see a clear path for how the small providers, small payers and small entities in the healthcare ecosystem would have the subject matter expertise or wherewithal to really take advantage of that.

Nonetheless, it is really thoughtfully laid out. I like the fact, as you mentioned, that it's agnostic to specific legislation or specific industries. And I like the fact that you have acknowledged the hooks into both domestic and international privacy regulations. Again, just a very impressive presentation, very impressive thought process behind this framework. Thanks.

Naomi Lefkovitz: Thank you. We absolutely recognize that issue with small and medium-sized businesses. Actually, as a result, we are this year working on some guidance for small and medium-sized

businesses to help them better use -- I say simplify but I always want to make sure that simplify doesn't get confused with not meaningful. We are looking at how do we sort of simplify some of the information but actually continue to make it meaningful for small businesses. We will be working on that this year thinking about the kinds of guides and videos and maybe a walk-through of where some of the essential points to think about in the framework could be for small businesses.

Rebecca Hines: Jacki, looks like your hand is up.

Jacki Monson: Yes, sorry, I was having some connectivity issues. A couple of comments and then I have a question.

We are one of the organizations that have actually used the Cybersecurity Framework. We actually report that to the Board, track program maturity and investments, and are now working on incorporating the privacy one. Although, I am not going to lie -- it was a little disappointing that we have different terms on the privacy side versus the security side. I would have loved to have seen them be the same terms but understand that not everybody is at that level of program maturity. I just wanted to provide that perspective.

I think the thing that I would love to see more of is the merging of privacy and security by design. We have a little bit of that but would love to see more of that and more of that forward thinking about not only how do we use the data but how are we set up. I think some organizations use the privacy impact assessments, they use security assessment, but actually designing it is the only way that we are going to solve the broader privacy and security problem.

Then my question is -- you mentioned a lot about adoption and trying to get individuals to adopt it. What is the game plan besides trying to partner with OCR and get some guidance out? And how can we help you with that?

Naomi Lefkovitz: One of the reasons for coming to groups like this is to actually -- You are the experts, and so we would actually want to take advice from you about where should we be going. Are there conferences, are there briefings or are there other associations that we should be meeting with? Honestly, we would really prefer to take guidance from you in terms of how we should approach the healthcare community. I was scheduled to speak at HIMNSS, for example, but obviously that couldn't happen.

Rebecca Hines: A question came across the Chat. Just confirming this is mappable with OCR's audit protocol.

Naomi Lefkovitz: I have to say I am not familiar with that. As I said, we worked specifically on the privacy rule and breach notice, but I haven't worked on that so I would have to inquire about it. Although, if you have more information, I would be happy to look at that.

Rebecca Hines: Rachel, would you happen to know?

Rachel Seeger: Yes. It doesn't map directly to the audit protocol, but I can share that OCR and NIST are in discussions about exploring a crosswalk to the HIPAA privacy rule from the NIST -- framework. Right now, we are all COVID19 all the time, but it is something that we have on our radar and we have been in great discussions with NIST and Naomi and her team. So, more to come.

Rebecca Hines: Very good. Naomi, thank you for taking the time to share all of this and I encourage the members to continue to help with dissemination and implementation. I think that is a really good role for this committee. If you at any time want to follow back with us, certainly you are always welcome.

Naomi Lefkovitz: Great. Thank you. We would love to. And if you have any recommendations for us we would absolutely love to hear them. Thank you.

Rebecca Hines: I will leave that note with the members of that subcommittee, Frank and Nick and Melissa and all of you.

Ed You is on detail to HHS through the FBI, and I will let you introduce yourself, Ed, because we have not actually met. Thank you very much for accepting our invitation and I will turn it over to you now.

Safeguarding the Bioeconomy

Ed You: Good morning, everyone. First, I want to thank the committee and Maya Bernstein in particular for the opportunity to present to you all. Very quick, I am a supervisory special agent in the FBI's Weapons of Mass Destruction Directorate. My responsibilities are to look at current and emerging biological threat issues, and, as was mentioned, I am currently detailed to the Department of Health and Human Services Office of National Security.

My responsibility is to look at what are the growing challenges, especially in the face of biotechnology. The reason why that is important is, when you think about biological threat issues, what immediately comes to mind historically has been the threat posed by emerging and re-emerging infectious disease and COVID-19 is a painful example of that. But it all boils down to dangerous pathogens and toxins.

But in the wake of the rapid advances in biotech I think it is important to note that we need to expand the scope of what constitutes a biological threat, and hence, the term bioeconomy was brought up, because where biotech is being applied is across multiple sectors, in health, agriculture, manufacturing and energy, with significant implications to our national economy. As a result, I don't think we are defining or assessing risk and the security challenges appropriately. As the slide says, there are amazing promises but then also emerging challenges.

As I said, one of the fastest growing areas in biotech health is in the health sector, and I am speaking to the right committee for this. A good example is the dawn of precision or personalized medicine. A whole element of this is identifying and aggregating different types of data from various sources, analyzing them and then coming up with new treatments, therapeutics, new products, and leveraging how you can not only identify but then utilize the data.

I'm glad I am following after (inaudible) presentation because now I get to bring in the national security or law enforcement perspective when it comes to health data. What I want to present to you is the thought process that data is basically the new oil. Data is going to be the new resource that many of the new technologies and applications are going to be built upon, dependent upon, and I'm just going to go around the horn and showcase where some of these data sources are coming from.

If you look at the top left in the human DNA helix, the first time an individual's entire genome was fully sequenced was the completion of the Human Genome Project in 2003. That effort took the US Government 10 years and $3.5 billion to get that done. That was then.

Today, you can sequence your entire genome in less than 24 hours, and just two and one-half weeks ago a company announced the ability to sequence a full genome for $100.00. So we went from $3.5 billion to $100.00.

What this means is we are generating massive amounts of genetic information. As powerful as genetics is, it's not quite enough because your genetics doesn't change much over the course of your lifetime, which is a good thing unless you happen to be a really big X-men fan. To supplement that, you need something called longitudinal data, and that is exemplified by the picture below the helix.

This is data that reflects what happens to you over the course of your life. This is exemplified by things like the electronic health record, insurance information, medical histories, family histories, and identifying what medical conditions has an individual suffered from or are existing, what treatments are provided, what drugs were administered. By aggregating the longitudinal data along with the genetics, analyzing that, you can come up with better informed decisions on how to treat disease conditions.

The government is leading this in two areas. One is the NIH's All of Us program, and the other example is the Department of Veterans Affairs' Million Veteran Program. Finding one million volunteers for each of the programs, get their genetics, volunteer their health and medical history and analyze that.

You go to the other part of the slide, the private sector is jumping onboard this area, too. Companies like Apple and their Health Toolkit. You download the app on your smartwatch, the sensors will track your heart rate. The different wearable technologies looking at your exercise, how much sleep are you getting, maybe the quality of your sleep. And the whole idea is monitoring your daily lifestyle to identify risky behaviors. Maybe you are not getting enough exercise or getting those 10,000 steps in. And mitigating those risks today in order to prevent the disease state from manifesting. It has really become a consumer-driven element to healthcare because I think they recognize that there is a lot of profitability at stake here.

There are multiple different sources of data coming from many different areas, and I don't think we really are appreciating their value, but now I am going to walk through what some of the potential security considerations might be.

Here is an example of direct-to-consumer resources. There has been an explosion of companies that provide direct-to-consumer genetic testing. The business model here is you pay a fee upfront, you send in a saliva sample, they will take DNA in the cheek cells, not the entire genome but I'm pretty sure that is coming soon, and they identify interesting or relative markers for the consumer, things like for women they will identify what BRCA gene you have to give you some idea of what your risk is of developing breast or ovarian cancer. And the all-popular genealogy studies, you know, I want to find out what percentage of this I am. I'm sorry I don't know what the draw is, but there are companies like 23andMe, Ancestrydna.com, very popular.

What you all should know is, in this example, 23andMe has I think a little over five million subscribers, but what no one recognizes is that that subscribership model for that company is actually a loss leader for them. They actually lose money. They don't turn a profit at all. So that begs the question, what is the return on investment. It's all about the data that they have access to.

They actually published a scientific paper in 2016 where they identified 15 genetic markers tied to severe clinical depression, and what's important to note here is how they were able to find this correlation. They were able to access a cohort of 450,000 of their customers, their genetic information,

and these individuals volunteered that longitudinal data, their health history and their family history. By utilizing that dataset, they analyzed it and they were able to find this correlation.

The important thing to note here is that this is one of the few occasions where we see a really interesting connection between data and a clinical state. But what I think is more important is how they found it. The fact that they were able to tap into a cohort of almost half a million compared to, say, for example, an FDA or NIH clinical trial study where you're lucky if you get a few hundred or maybe a few thousand volunteers. But the way this model was set up they have ready access to a large number of participants, and what this does is now they have insight into a potential drug target -- treat depression. That's the whole name of the game.

In fact, about two years ago, 23andMe made a large investment in themselves to expand a business not in DNA diagnostics but in pharmaceutical design and development. They actually tipped their hand when in 2019 GlaxoSmithKline invested $300 million in 23andMe, and what this investment did was to allow GSK to mine all the data that 23andMe has in their holdings.

Ultimately, again, it is all about identifying new drug targets. But here's the thing. In looking at their analysis -- and they were able to come up and design a potentially blockbuster drug to treat cancer, diabetes or depression. Great for the companies, but those five million or so consumers, what they don't realize is that when they sign on that line and onto these services, they sign away any rights, any claim to the products that the companies are able to derive from their data. So, despite the fact that it's their data contributing to the product, they don't have any claim to it. Nothing wrong with it, but it really begs the question do they really understand where their data is going.

The bottom line is this is the new norm. This is the business model that's coming up. It's all about what access to data can a company have and how can they turn it into a commodity. The upshot here is that whoever develops the largest, most diverse dataset is truly going to own the day and it will truly be something powerful and incredibly profitable.

Unfortunately, I think the adversaries and bad guys know this, too, and I want to propose to you that that is why you're seeing significant targeting of the healthcare sector with cyberattacks. I listed some of the prominent ones over the last few years -- Community Health Systems in Tennessee, 4.5 million patient records. Anthem Blue Cross, that was epic, 80 million. Premera, 11 million. UCLA, 4.5 million.

The one thing I want to note here is the impact. We are talking about a significant percentage of the US population. The other part I want you to note is that all these hacks were identified to have been perpetrated by a Chinese-based hacker, so these records and information are residing somewhere in China.

In the wake of these hacks, what have been the immediate security concerns? It is, of course, the loss of PII, the possibility for identify theft, the possibility for insurance fraud. I get it.

The challenge, though -- If you look at this one press article where in one of the intrusions they identified the parts of the networks that contained medical information, and insurance claims were compromised. When I saw that, it really was a punch to the gut because what this exemplifies to me is access to what I said before, longitudinal data.

So you're telling me that sitting somewhere in China to the tune of millions of Americans is insight into an individual's potential, current and prior medical conditions, what treatments have been

administered, what drugs were provided, what the drug course might look like. So, not only potential insight into ongoing drug studies or clinical trial information but some really relevant longitudinal data.

If 23andMe can find an interesting connection to a clinical condition from a cohort of 450,000 individuals, then what can China potentially do with tens of millions of such data points that are biologically relevant?

Here, what I want to share with you all is I think it's important to note that the biologically relevant data is far more valuable, has far more consequence than any of the potential privacy issues here or the fraud angle. We are just not assessing it that way. I also don't think we're looking at cybersecurity in the right context in this space. And it is ongoing not only in the US, but these Chinese intrusions are occurring all across Europe, everywhere else in the world. So I classify this as China's ongoing covert or criminal acquisition of health data, but unfortunately, I'm afraid to say that we are also giving it away.

What I mean by that is that in the last decade or so China has heavily invested in the DNA sequencing market. Here is a list of companies that have come on the scene in China and they offer large-scale DNA sequencing at low cost. They very easily out-bid a lot of our domestic companies. They have subsidies or support from the Chinese government. Many of these companies are CLIA and CAP accredited, they are HIPAA-covered entities as well. As a result, many institutions across the US have partnered with these organizations in China to do their sequencing.

You see BGI on there. They are a giant. For example, the Fred Hutchinson Cancer Research Center announced last year that they are engaging BGI as a strategic partner and BGI is going to be sequencing all of the Hutch's cancer and pediatric samples. Mt. Sinai, Johns Hopkins University, the Mayo Clinic, they have all contracted or partnered with BGI to do sequencing. So, all across the US we are sending to these companies, tumor samples, biopsy samples, blood samples, again, because they meet all of our existing privacy criteria and they offer the lowest price point. Yes, our clinicians and our scientists get the genetic information, but at the end of the day, they have it, too.

It is not just in the US. That company, BGI, also went into an agreement with the European Union back in 2014, and with this agreement they rolled out a non-invasive prenatal test kit across 16 European countries. Currently, if you are an expectant mother and you want to check on the health and welfare of your future child, you undergo an invasive, somewhat risky amniocentesis. Well, with this new BGI test kit you just do a blood draw from the arm of the mother, they will isolate the circulating maternal and fetal DNA from the placenta, sequence it, and you get almost the same results as you would get from an amnio. It's faster, it's cheaper and it is definitely safer.

When they rolled this out in 2014, they were able to get 400,000 pregnant women enrolled in the program. As of about two years ago they have more than 2.5 million. That's 2.5 million across these 16 countries. And what I want to note here is that you will see that England and Germany allowed this test kit in, and I highlight them because those two countries have some of the most robust privacy laws in the world, and despite the fact that the EU rolled out the GDPR, because this is a clinical kit and, again, they meet all the privacy criteria, it undercuts all those so-called protections.

And here is where it gets a little more insidious. BGI actually published a scientific paper in Cell where they took that non-invasive prenatal test kit from 140,000 Chinese mothers and they went beyond the prenatal test panel, so they went beyond just checking for cystic fibrosis markers or (inaudible); they actually did whole genome sequencing, and in doing so, they were able to tease out some interesting and unsettling information. They were able to identify the ethnic makeup of the population and then

even more intimate information. They were able to identify prior viral exposures that these mothers had suffered from. So, some very personal information, and this is from a non-invasive prenatal test.

The theoretical question here is if they were able to tease this out from 140,000 Chinese mothers, what could they potentially glean from 2.5 million mothers across Europe?

And why this is important -- This is a press release that came out in February last year where Thermo Fisher, a large US biotech firm, announced they were no longer going to be selling DNA sequencing equipment to China because they found out that the Chinese government was doing something pretty sinister. The Chinese government had rolled out a program called Physicals for All, this low-cost medical exam, and 36 million Chinese participated in it. Thermo Fisher found out that the Chinese government was utilizing this DNA from the collected clinical samples to identify ethnic Uighurs.

For those of you who are not familiar, Uighurs are an ethnic minority in the western region of China. They are predominantly Muslim. There have been multiple stories about how the Chinese government had been trying to displace the Uighurs from their land and from their businesses and have been corralling them into what they call re-education camps to the tune of hundreds of thousands of Uighurs.

So, have we inadvertently, unknowingly, unwittingly provided not only the technology but potentially the expertise to enable the PRC to conduct what I call discrimination in high definition? But this also focuses on the point that it's not just about privacy. It's looking at what happens when you have an authoritarian regime, a foreign entity like this, that has access to health-related data. This is taking it way beyond the pale on what some of the privacy challenges are or how we define privacy.

There is another company besides BGI called WuXi Pharma Tech, another Shanghai-based Chinese firm that has very broad resources. I showed you that really nice example of proof-of-concept of what 23andMe can do when they get enough data and tie it to depression. But a year before they came out with that publication, this company, WuXi, invested in 23andMe. So why bother stealing the data when you can absolutely legally, above board, with complete legitimacy just invest, acquire or merge with a company that has access to health data?

Again, it begs the question how many other companies like this have foreign investments, and, more importantly, how many consumers understand that when they sign onto these services? Do they have the information to understand and recognize where there data is going, how is it being stored, how is it being utilized but, more important, who has access to it?

The bottom part of this slide I have gone on record as saying it just quite frankly pisses me off that WuXi acquired their own DNA sequencing company called NextCODE, and their operations are also based in Shanghai. Again, they are able to do large-scale DNA sequencing at low cost. WuXi NextCODE is CLIA-CAP accredited. They are also a HIPAA-certified covered entity. They are even FAR and DFAR-accredited so they can put in bids for government contracts. They meet all of our existing privacy regulatory requirements, and also, because they offer the lowest price point, in this press release the state of California at a state level has gone on to even license them.

What this means, though, is if you are a resident in California and you go in for a medical exam and you require genetic testing, you sign the HIPAA consent form and, despite the fact that you might think your health data is going to be kept private and secure, because this foreign company meets all the existing criteria, your samples are going to be sent overseas for processing.

So, from a privacy standpoint, as I said, they check all the boxes, but from a broader, national security standpoint it just begs the question are you kidding me. And this is what's happening in California. I don't know what is happening state-to-state because you are all probably aware that this is a patchwork. But if you're a contracting officer, how would you know any better?

In this slide I showcased that this entity WuXi has access to companies that have genetic information, potentially some longitudinal data as well as now genomic information, but if you go to the next slide, this is the other shoe dropping. WuXi announced last year that they are building a vaccine production facility. So could they in fact be accessing the data and analyzing it and be able to turn that around and start developing vaccines? This place, they haven't even finished construction yet and they already have a 20-year, $3 billion contract in place. The running joke here is that I hope it's not DOD or BARDA.

The upshot here is China already dominates the global generic pharmaceutical market, and most of the API that comes from our drugs comes from China. Are we also inadvertently giving them the building blocks to gain entry into the vaccine market as well? Especially in light of what's happening to us right now with COVID19 -- which I will talk about later because there are bioeconomy implications with the current pandemic -- this showcases how shortsighted we have been. More importantly, are we not recognizing the true nature and value of health data, especially when it comes from a national security standpoint?

This gets even more interesting. The two companies I just mentioned, BGI and WuXi NextCode, these two giant data-sequencing firms, both in China, both presumably competitors, both announced strategic partners with Huawei less than a year apart from another. Huawei should always get your attention a little bit. They have been in the news quite a bit from a national security standpoint. But on its face, it sort of makes sense that if you are generating massive amounts of genomic information you're going to need to partner with a company like Huawei, this telecommunications company, that has the technical infrastructure to house and process large sets of data. So it makes sense.

But this slide, this is a different shoe drop, show that Huawei, with these strategic partnerships with these Chinese DNA firms in the backdrop, announced in 2019 a formal partnership with Philips Healthcare. This scares me because in this partnership the goal is to aggregate patient electronic health records, patient insurance and medical histories, genetic data, medical imaging data, even EKG, EEG scans and even wearable technology like FitBit data uploads, and basically build out a very large multifaceted dataset and leverage their artificial intelligence and cloud analytics, and roll out customized, personalized and, most important, low-cost patient healthcare delivery.

They have already implemented this in several hospitals across China and the early indications are that it looks like it was working, that Chinese physicians are actually able to utilize patient health data and the analytics that went along with it to help better inform them on the best treatment.

So, if they are able to improve healthcare at lower cost, what is to stop Philips from bringing that to Europe? What's to stop Huawei, for example, from partnering with, say, Kaiser Permanente here in the US? With the data that they have on the back end, can they offer, promise and actually deliver low-cost, customized patient healthcare? How do we say no to that? Would we be able to say no to that?

So, as I mentioned, China already dominates the generic pharmaceutical market. Are we giving them access to the vaccine market? Are they posturing themselves to be able to actually provide low-cost healthcare? That is the whole ball of wax.

The nightmare scenario that has evolved for me -- and it's no longer from a biological threat issue -- is the science-fiction based, well, someone is going to use CRISPR-Cas9 and engineer a virus that causes the apocalypse. That is traditionally how biological threats have been conveyed. But from my standpoint now from a bioeconomy standpoint, the nightmare scenario is that we are going to wake up one day and because of our shortsightedness and lack of understanding of the true nature and value of data, we are going to realize, hell, we have just become healthcare crack addicts and China has become our pusher. What happens if we become completely dependent on a foreign supply source for our pharmaceuticals or vaccines or therapeutics or healthcare delivery?

Not only does that mean co-opting of an entire market share of business models, but that also means our entire job opportunities are going to be transitioned there. Do we understand what that means in the long run?

So that has been my nightmare scenario. I hate to say it, but the nightmare is sort of becoming a reality. In April of last year, the Defense Department awarded Philips Healthcare a $450 million contract to look at patient healthcare delivery for all four branches of our military. Without having a robust understanding of the contract process, did we just give Huawei backdoor entry through Philips Healthcare access to our active duty members' medical records? This is not cyber intrusion, this is not hacking, this is not ransomware, but again, this is a different type of vulnerability.

And I mentioned before, if you are a contract officer how would you know any better? You're going to go through the checklist. This company is FAR and DFAR-certified, check. Are they HIPAA compliant? Check. Do they probably meet or exceed NIST cybersecurity guidelines? Check. Do they offer the lowest price point? Check. CLIA-CAP accredited? Check. But unless you have a broader understanding of the context -- I don't know how many more of these types of contract exist across the federal government or at a state level.

I have just showcased that China has set themselves up to get data from all around the world. It's important to know that it is basically a one-way street because China has enacted laws that went into effect July 1 last year where the Chinese government is absolutely clamping down on the sharing of biological material and data. Now, if you go into a contract relationship or partnership with China you have to have a hosting Chinese institution. You can look at the last article, that any data or patents that derive from the collaboration, that Chinese institution has first right of refusal for ownership.

What's also important to note here is that with this new law, any US entity that's partnering with a Chinese firm or any US entity that might have an extension of their business residing in China -- because, for example, data storage is cheaper over there -- despite the fact that it's, as I said, maybe HIPAA-certified and all of that, this new law allows the PRC, any Chinese law enforcement or Chinese intelligence agency the absolute authority to be able to access that data if they deem that there's a security necessity.

We just did a presentation -- we're trying to do a lot of due diligence on our side of the house and for the companies, but do our vendors, our universities, our medical providers really understand what's happening on the other end when they go into these partnerships with China. I think it's really important and incumbent upon us to do our homework to understand what the legal landscape in the countries is where we are doing business, and understand what the risks of that entail.

There actually has to be a balance, especially when it comes to the bioeconomy. We need to make sure that we not only address security but also support innovation. You will note that I did not say we need

to shutter companies like 23andMe. Actually, those are the tip of the spear when it comes to innovation. I did not say we should stop data-sharing altogether. That doesn't work in biology, it doesn't work in a healthcare crisis like we are having right now. But we absolutely need to strike a balance. It is not just about making the other guy -- slowing them down, but it's also how are we enabling ourselves to run faster. How do we make sure that we stay the leaders in innovation and R&D?

So, how did we come to this perspective in the first place? I hosted a series of workshops first with AAAS and then with the National Academy of Science and at these meetings brought in representatives from places like Amazon, Google, Intel, IBM, Microsoft, Dell and challenged them with, look, this is where the US economy is going with biological data. Where are we with national security? And there was a unanimous response that we're doing a whole lot in privacy policy, particularly when it comes to clinical data, but from a national security standpoint we are not doing a whole lot.

We generated these short meeting reports that are publicly available. They became very important outreach tools for us. We conducted engagements. We actually helped change legislation to the point where, in this example, this Chinese firm iCarbonX -- this is a Chinese firm that focuses on artificial intelligence and machine learning tools development -- they had invested $100 million into this organization called PatientsLikeMe. PatientsLikeMe is a US organization that's a social media platform. It is basically the healthcare version of Facebook where you have individuals, about 750,000 or so, who share on a daily basis what medical conditions they may be suffering from, what drugs or drug trials they may be participating in and sharing the drug reactions and the efficacy. So there is some pretty intimate information.

When this Chinese firm invested, it kicked off a US Government review and we identified the vulnerability to the point where President Trump ordered the divestment of iCarbonX from PatientsLikeMe. In one sense, this is a home run because it's taking out a foreign entity from gaining access to US persons' sensitive data. It puts the healthcare sector on notice about the value of their data, but the downside is that it's a shame that an organization like PatientsLikeMe has to resort to looking for a foreign entity for investments. Where is a domestic company that would be willing to step up and invest in them as a strategic partner to make this happen? That is what I mean by where are we striking that balance.

Congress is waking up as well, too. This is a letter that was signed by both Senators Rubio and Grassley that was sent to HHS CMS. There's a quote on the bottom that is straight from the letter, "Taxpayers cover the costs of CMS payments. Accordingly, they have every right to know if their money…" (and their data for that matter) "… has gone to entities connected to the Chinese government."

The Department of Defense has woken up, too. They put out this memo to all their active duty members warning them about the risks associated with participating in commercial DNA test services.

Ultimately, this translated into a formal National Academy of Sciences consensus study report. This was a full-year study. If you look at the right column, the very diverse section of the National Academies, this doesn't happen very often. Usually, these types of studies are just taken up by one board or division, but because the bioeconomy touches on multiple areas not only did different parts of the National Academies participate but they convened a diverse set of experts for their committee ranging from biologists, agricultural experts, economists, foreign policy experts, to look at how do we define the US bioeconomy, how do we scope it. They ultimately came up with some formal policy recommendations

for how do we better protect and promote our bioeconomy. This just came out this past February, which is awesome, and I highly recommend that you all look at this.

This is the ongoing COVID19 implications from a bioeconomy standpoint. Again, I don't think we're looking at it through the right lens. I am going to walk you through a timeline. When it first came out in the US we were trying to rapidly be able to ramp up diagnostic testing. CDC had some major challenges in getting a test kit out to public health, so that delayed things. What it did was created a vacuum.

Guess who stepped up to fill that vacuum? That company, BGI, that I mentioned, rapidly rolled out their own coronavirus diagnostic test. It is two-pronged. One is RT-PCR based, which is a decades-old approach but it's the one that CDC is offering. The other test is whole genome sequencing, which is much more up to date. The thing is, as soon as they developed it the Chinese government gave them emergency use approval in China, and the very next day Europe jumped onboard to gain access to both of those capabilities.

Interestingly, BGI, the company, not the Chinese government, not a hospital, but this private company built a high containment laboratory hospital in downtown Wuhan in five days, and this hospital was able to process 10,000 clinical samples per day.

So it's not just doing DNA amplification of the virus, but they were able to do whole-genome sequencing. It means that they have some even better insight into looking at virus-host interactions, which gives them a tremendous edge because we're not seeing any of that data, by the way. We are working off of the few hundred patients that we have here domestically.

By the way, most recently, too, that same diagnostics test got CE marking by the European Union which means that they can come into the commercial market. I need to update this for you all because as of last Friday, this BGI test kit just entered into the US market. As a matter of fact, there was a press release just this morning that Baltimore just received 1,000 of these test kits, and that is just a start. Then you have a strategic partnership between BGI, Intel and Lenovo, to leverage their machine learning capabilities to come up with new drug targets and then better characterize the virus-host interactions.

What this means, though, is that this company, WuXi, announced that they can go from DNA analysis to an IND candidate drug in four to five months. So, less than half the time it will take us to come out with a counter to the pandemic.

What I'm afraid is happening is that there's a ticking time bomb. I understand we are trying to do our utmost in looking at privacy, but unless we have a broader understanding from the national security standpoint and from the bioeconomy, we are opening the door for an entity like China to be able to dominate in this space. Are we giving them the keys to the kingdom if we don't understand the value of our data today?

The thing is the data in residence may not mean all that much now, but if you aggregate it enough later on when they get true AI or true quantum computing, they are off to the races. They won't have to steal our IP anymore; they can just analyze and generate their own.

And it's not just China in this space. We have to also be on the lookout for countries like Russia and Iran. Honestly, I think in 5 to 10 years we are going to be in the same boat with regards to India because of their own population growth, their aging population, their own healthcare needs. They are going to

make this bioeconomy work for them as well. So, are they going to be competitors, or could they potentially be strategic partners?

Again, I just wanted to give you a different perspective for looking at health data security and an understanding of what the potential bioeconomy implications are.

Rebecca Hines: Thank you. That was different than any presentation I believe this committee has received, and you brought a whole new angle to our Subcommittee on Privacy, Confidentiality and Security, so thank you.

I would like to open it up. Melissa?

Melissa Goldstein: Hi, Ed. Thank you very much for that wonderful and very thorough presentation. I would like to ask you to outline for us -- you used the word "insidious" several times, which I take to mean danger or evil, add your own adverb. So I am wondering, are you worried about anything the Chinese government might do with data, anything the Chinese companies might do with data? Is there any stratification among the companies perhaps? And are you worried about US companies or US patients depending on Chinese companies?

And have there been any actions, any usage of data by the Chinese companies that American companies are working with which have given us signs that say stop now? We know what China is doing with its own population, right? What I'm wondering -- and I understand the Chinese bio law right now. I'm wondering if there is anything to pin our privacy concerns on other than generalized information about China.

Ed You: That is a tough question and my general answer is yes, we need to be concerned about all of the above. I will tease apart your question.

First, I don't think you can delineate the difference between a Chinese company versus the Chinese government. They are one and the same. You cannot operate as a company in China without some specific ties to or support by the Chinese government. There is no individual enterprise there, no private entity. And if you want to be able to operate, you are going to have to have Chinese government to back you.

The reason why I use insidious, I noted in specific parts of my presentation, for example, how they utilize genetic information to identify the Uighurs within their border. The challenge, though, is things like even our own individuals here in the US who collaborate with China don't understand that that is what's happening on the back end, that that is exactly what the government is doing. The problem here is that we haven't had the smoking gun yet. That is the problem.

To your point, what I'm afraid of, what scares me, is that by the time we have the wake-up call it's already too late. If we wake up and, as I said, we say, hell, we have just become completely dependent on them for our future vaccines or our future pharmaceuticals, then it's too late. I use the terminology that I think we are in the middle of a biological space race, and shame on us for not recognizing that that is happening.

Why that's important to note is that it showcases that this is a whole of government, whole of academia, whole of private sector, whole of society issue, and also it's because of the challenges we haven't just been given that Sputnik launch wake-up call moment yet. But my feeling is that the timeline

is rapidly shortening when we are going to probably get that wake-up call moment. Maybe it's going to be the fact that China comes up with -- that they will be able to come out of the COVID19 pandemic faster than anybody else and say, hey world, we have got the definitive test. And, oh, by the way, we also have a comprehensive treatment for coronavirus.

But by then we are not going to be in a position to be able to say no. They might be able to be in a position to take care of their own population better than ours, or withhold it maybe, because they want to take care of their own first. There have already been examples of that happening right now. For example, the N95 masks. 3M, the US firm has two factories in China. They were basically co-opted by the Chinese government and the masks that they were rolling out 24/7 the Chinese kept for themselves first.

Same thing happened with Gilead and their trial drug. They had put in a patent two years ago, but China put in their own patent for their (inaudible) to treat COVID19, and Gilead had to go with it. We are already seeing indications of it. What I'm trying to walk you all through is that this is a much broader scale, and we really need to assess risk in a much broader context, not just privacy.

I hate to say it, and this might offend some of you, but in the meetings that I had with some of those experts, their running theme was that privacy is a moot point. Privacy is dead. What we really need to start thinking about is to look at it from a national security standpoint. As things keep on evolving, as you wear the different wearable technologies, it becomes very hard to really look at understanding what does privacy even mean in this space. But we actually need to overlay it with national security to get a better understanding of what's important, how do we prioritize from that standpoint.

Melissa Goldstein: I am wondering what your policy recommendations are. What is the "therefore"?

Ed You: First off, I highly recommend looking at the Safeguarding the Bioeconomy, the National Academy study report. They actually did a very thorough deliberation, very nice job defining what the bioeconomy is, how we should take a first step in explaining it in the first place, and they actually came up with some formal policy recommendations.

I think one of the first things is realizing that we have got a problem, and then understanding it is not just about becoming complete protectionists. There are going to be some elements of it, but, as I alluded to, that doesn't work in the healthcare space especially in the wake of a pandemic. But it does also mean that we have really got to understand where are we leveraging our resources and investments to make sure that we are in a position to maintain leadership in the bioeconomy space. That is a challenge.

But I hope what I am giving you all is a different data point. Let me just give you one anecdote. I have given this type of presentation to different conferences including the AHLA conference, so I got a chance to provide this perspective to literally hundreds of chief security officers out there and they get it. The problem is when they go into the C-suite they don't get any place because why? The COOs and CFOs are saying no, we are not going to give you more in resources because, one, we don't see the return on investment and, two, the government isn't requiring us to do it.

But the important point here is that if you provide the bioeconomy standpoint where you take in biological threat issues and tie them to the economy in a way that has never been done before and showcase the impact, this is a really important way of showcasing to the C-suites that it's absolutely in

their best interest to start thinking about security at this point because, otherwise, they may not have any market share. You might not have a business in a few years down the line.

That is a little more substantive in your discussions and arguments than some of the regulatory requirements. Not that I want to downplay regulations; they actually serve a purpose, but I think it has to be a part of the broader discussion of what's at stake.

Melissa Goldstein: Thank you.

Frank Pasquale: First, I want to say, my name is Frank Pasquale. I have written a bit on some of these areas of preparedness. I wrote a piece in 2014 that cited articles stating that America could be short 600,000 ventilators. Sadly, that piece sank like a stone and was not very widely cited, so I sympathize with someone who is sort of warning about long-term threats because I do think that's really important.

The question I want to ask and just push back a little bit on is I think that looking at -- One of the other things from a political economy of healthcare perspective I think we have to acknowledge in the US is that we have a system that is largely governed according to short-term financial results whereby we disincentivize a lot of investments in long-term projects just by virtue of the way it's financially structured.

So I think that for the foreseeable future China may be the best hope for much of the world and for us in terms of developing some of these technologies. Therefore, I think an alternative here is not to deny the data necessary to make therapeutics, but it's rather to condition deals so that anything created there is available in the US on a fair, reasonable and non-discriminatory rate. That FRAND is something that I think is quite -- it's a big part of patent law and patent jurisprudence, and I think it could be applied here as well.

I was just wondering if you think there is a cooperative? I know in game theory there is both competitive and cooperative games, and I'm wondering if there might be a cooperative approach here whereby rather than trying to block access to very important data, which is what some leaders in Indonesia were actually attempted to do during the avian flu epidemic in the 2000s, instead going the path of trying to have CIFIUS or others condition access on the sort of fair, reasonable and non-discriminatory rate idea.

Ed You: No. I completely agree with you. You are not pushing back at all. But the problem is that, yes, I can say stop sharing data; the problem is they are not sharing theirs. It's a one-way street.

The point is -- I call myself a recovering biochemist because my background is in biochemistry and molecular biology before during the Bureau, and so I absolutely understand the nature of biology in healthcare; it's all intrinsically built upon and dependent upon the open sharing of data. But the problem is if we are the only ones doing it, what's the point.

I completely agree there has to be some level of reciprocity at the very least, but I think more near term and probably more reliable -- you already touched on it -- is that, as we go into a partnership, collaboration or contract agreement with a Chinese entity, or any other entity for that matter, go into it with our eyes wide open. Understand what the risks are, because we're doing so much or trying to do so much on our end to do our due diligence, but I don't think we are doing enough.

One, we don't recognize what the broader risks are, and we are not able to do the same kind of assessment on the other side understanding what when you go into a business with a country like China,

do a really good risk assessment. What does it mean, what is the political or legal landscape of conducting business or having an arm of your business in that kind of country.

Again, it is not just looking at privacy protection, but what's the point if you have that and then that particular foreign government has the authority to access that data whenever they deem it necessary. What recourse do we have?

Go into this with eyes wide open and either through contract terms of agreement or other types of stipulations do what you can to protect yourselves. But you are not going to go through that effort unless you understand what the broader issues are, and that is what we're trying to do, just trying to push out as much broad awareness as quickly as possible.

Frank Pasquale: Thanks.

Rebecca Hines: Vickie, you have your hand up?

Vickie Mays: Yes, I do. Thank you for your presentation. I want to ask a couple of feasibility questions. There are two issues that I am trying to understand. One is, when we do studies and we have applications that go through our IRB, it would be very helpful if there was a way for the IRB or for the investigator to know that if they contract with this group, X would happen, and so everybody then is forewarned.

I'm trying to get a sense -- It probably took you a lot to be able to track these trails. Is there any way that we can get this information in ways in which when we are conducting research or activities we can make sure that people are forewarned?

My second thing is, is it feasible within use agreements when we're using a test kit, that that should be a part of it, to tell us all of the uses that are possible and the connections between the company itself and where that company may literally be sharing the information, even if it's de-identified, that they may be sharing that information, so that we would know that?

Ed You: For the first part of your question, that is why I used the space race analogy, that this is an all hands-on deck issue. We are looking at a layered approach. That means you have to have institutional buy-in, so not only do you have to have buy-in at the administrative level, then all the way down to whoever is developing the contracts, then all the way down to the IRBs, and to the actual PIs and even actually to the volunteers or patients that are participating as well.

As a consumer, if this becomes your medical diagnostic, then as a consumer who is taking the time to look at the end user agreement when you download that app to access your data and taking the time to understand this is where your data might be going and how it might be used.

Vickie Mays: How can we get it? That's what concerns me. The consumer I think is willing to do it, but how can we make sure that we can get it?

Ed You: Right, and that is the thing. I am happy to report that Congress is understanding this so they have legislation to look at this. The White House is looking at the bioeconomy as well and trying to push out the ability to educate the population on the promise as well as some of the security challenges when it comes to this space.

The biggest challenge I just sort of touched on is how do we get this information out as quickly and as broadly as possible. That's one of the reasons why I am so grateful for the opportunity to be able to present in forums like this. Again, thank you to Maya Bernstein for the invitation and the opportunity.

If this resonates with you all, then you are now part of the solution in helping to raise awareness. Until we are able to get the policies in place and until we can get the National Academy's reports out, maybe it just starts with your direct conversation with an IRB member or with a contract officer and just start that awareness piece going.

I am happy to report that there have been some best practices that have been implemented. I am aware of one statewide healthcare network who made the business decision to not allow any patient data to go overseas without first some level of risk assessment being conducted by the organization leads, because they want to know where and when is the patient's data going because they have determined that that does pose a risk to their patients. And they went even beyond that. They made it so that all their contractors, subcontractors and business associates have to abide by that business decision as well.

So they took that step outside of any existing policy because when they heard this message and they conducted their own risk assessment they determined this is the right move to make in the interest of their patients.

So we are starting to get there, and I think as more and more best practices are getting developed and implemented we need to share those as quickly as possible. It's not just about the awareness-raising and scaring people straight, but it's also helping to come up with good ideas and be able to address some of these challenges.

Vickie Mays: Thank you.

Rebecca Hines: Denise, you are still on mute.

Denise Love: Okay, I have a mute problem. Thank you for this wonderful presentation which is overwhelming as far as action. There seems to be a proliferation of clinical trials, so, along the lines of what Vickie was saying, are there red flag warnings that we should tell people to look for, or guidance? Because I am at the age where I'm getting invitations all the time for clinical trials for all sorts of drugs and agents and it seems endless.

But what should a consumer look for, or what should we tell them to look for in these?

Ed You: Something that I personally started doing and I think I really upset my physicians, is that when I get those HIPAA consent forms -- take the time and effort to go through those lines and understand how your data is going to be utilized.

Just anecdotally, I took the time in one of my most recent doctor's visits and went through the HIPAA consent form. There was one line saying that by signing this I am allowing my information to be shared for research purposes, and it wasn't clear exactly what usage. They just threw in the de-identification aspect of it.

When they weren't able to explain to me where would it go type tracking, I asked if I could opt out of that particular part of the agreement, which threw them for a loop because they said in the two decades

they had been in practice, one, no one had ever taken the time to actually read the whole thing, and two, they didn't even realize that that was part of the agreement.

So that is a little bit of an issue. It does mean go into these things with eyes wide open as much as possible. Because what I have done and I hope I have succeeded in, is just expanding the scope of what constitutes risk for us as patients and as consumers.

But here is another thing I want you all to take into account, too. It is not just about us. It's looking at our US bioeconomy ecosystem versus like China's ecosystem. I can tell you right now they are probably conducting a whole slew of clinical trials, and are we ever going to see that data? Do we really know what's happening, what is the quality, what type of IRB review are they going through over there? I hazard a guess -- and this might get me in the hot seat, but -- I really wonder if it is up to snuff compared to how we do it here in the US.

My concern is that we do so much and with good reason, in the interest of patient protection and privacy, but we also need to step back and see how does this compare to their ecosystem. How is this advantageous for them? What are the challenges for ourselves?

Another example is say, we have a clinical trial or even before the clinical trial we have a candidate drug that we want to test in an animal model. Well, you would be hard-pressed to be able to conduct nonhuman primate research tests here in the US because it has been very expensive, a lot of regulatory rules. Guess where it's easy to do it? China. China has set themselves up to basically dominate the global nonhuman primate testing market.

The cost of doing tests in monkeys is much cheaper over there. They have streamlined their own regulatory process to get it done, and they have expanded where they have breeding programs where they can do hundreds of thousands of monkeys very easily. So it's basically kind of the field of dreams for them, that if you build our PIs then drug companies will come to test out their candidate drugs or treatments.

So we have to look at it from end to end, and we have to look at it holistically that way, so, ranging from an individual patient level all the way down to looking at it from an institutional clinical trial all the way to a private company looking at different drug developments to finishing as well as from a government policy standpoint, and doing a holistic comparison between our ecosystem and how we conduct research and healthcare delivery versus theirs, and understanding where are the pressure points we need to address and negotiate.

Denise Love: I have long advocated that people need, on those HIPAA consents that you reference -- that it's their duty to permit *bona fide* and appropriate research purposes, so we don't want a chill to have our own people for our own research pull back out of fear. I don't expect an answer, I'm just saying we need to strike a balance where people are comfortable with their data use downstream for research but appropriately, and what that distinction is.

Ed You: Completely agree with you. This is one of the recommendations that came from the meetings that the FBI convened. One, for example, is why don't we have a core domestic capability to do large-scale DNA sequencing. Why are we putting our PIs and research institutions in a position where they have to go offshore to get low-cost DNA sequencing? It is not all that difficult to have a sequencing center of excellence here in the US where it would be able to do DNA sequencing quickly and at a low

cost. The problem here is it requires strategic thinking to make that investment to make that happen. And that is just one example.

To your point, if we had the wherewithal to understand what the broader issues are then we can make those specific strategic investments to make that happen so that when you do conduct these research experiments or clinical trials we have a domestic core capacity to be able to do it in the spirit of patient privacy or human subject protection. Also, taking those same standards and expectations abroad when we work with a foreign partner.

That's what I mean by it can't just be protectionist. It also means that we must make the right investments. And this was coming from those recommendations I mentioned. We absolutely have to have a strategic perspective and, therefore, look at where do we make the proper investments. It is not just about the exfiltration of data but it's also the very real opportunity costs, the missed opportunities that might be presenting themselves.

Denise Love: Thank you so much. I think you are singing to the choir here. This is great stuff.

Rebecca Hines: This is really good, and I don't want to cut us off so let's go until 11:00 and we will take our break at 11:00. Alix?

Alix Goss: Yes, thank you. This has been an eye-opening and really interesting conversation. We have had a number of touch points throughout the discussion relating to citizen involvement, education and awareness, and that has been an ongoing theme within the Privacy, Confidentiality and Security Subcommittee's work in data stewardship. There has been this ongoing dynamic of the responsibility of citizens, and the HIPAA consent form example really brought this home for me.

I ask those every time I go. My husband recently went to get new eyeglasses and they wanted him to sign a form and I said he hasn't gotten the form. Can I see the form? And of course, they looked at me like I had three heads. She went to find it and 10 minutes later I said to my husband, who was looking rather irritated, are you going to sign it anyway? He goes, yeah. So I went over and told her to stop looking, but this is serious stuff. And she just looked at me again like I had three heads.

We have this situation where we need to, as a committee, look at what we can do to try to infuse an education level, and we have been working really closely with OCR -- and I appreciate the videos and the consumer-facing content that they have developed to simplify this, but we need to get all the language and legalese down in plain English. When we think about level of education and reading benchmark that we need to strive -- you know, I spent my first 15 years working in Medicare and working in appeals, and let me tell you, I have what's called fogged content down to a fifth and eighth grade reading level more than I ever really want to.

And so I think this is not just a business matter, strategic thinking matter, it is an education matter. We have to become active participants in all of this. And what I really would love to see us, as a committee, think about is (inaudible) beyond the think tank, kind of big policy perspectives, but how we can help bring this down to the point, whether it's standard curriculums so we can also have the young-uns of the world to help simplify this and help protect our elderly who may not understand all the technologies and implications when they are just trying to get the help they need to be healthy and happy.

Ed You: I really appreciate that. As a matter of fact, I was a guest speaker for my son's ninth grade biology class, and the teacher really was galvanized as -- I kind of mentioned it before -- that this is going

to become a health tool, a diagnostic tool. And the younger generation, you would be hard-pressed to find them without this. What are we doing to equip them to become responsible digital citizens and help them understand that the relevance of their data -- it's not just a privacy standpoint but looking at how their data could potentially be co-opted or subverted for uses that they may not have considered?

Especially in the dawn of the Internet of Things, for example, in this year of 2020, every Ford and GM model car is going to have some form of biometric data capture and transmission back to the companies. You have to actively opt out of it when you purchase the car. Otherwise, as soon as you Bluetooth connect your smartphone or the different data capture the car has to prevent you from falling asleep at the wheel, for example, or how hard you're braking, ultimately that is going to have some sort of biological application. They are going to look at how do you monetize that data to potentially sell it to a franchise that, based on your driving patterns, you should put a gas station here or a convenience store here. That is marketable, and they can sell that.

But that is biologically relevant data and has security implications as well. Even at that level I don't think people really understand. And in the rapid chase for ease and comfort and, also, decreasing costs, we are giving up a lot not only in privacy but I really think we are rendering security really short shrift.

Alix Goss: It is even more important as we think about creating more data liquidity and interoperability to really (inaudible) the data aggregation from multiple sources to help address not just medical dynamics but also the social determinants of health. These little IRB implications, procurement implications that we have been talking about over the last hour are really critical for us to think about how those tentacles of awareness need to really spread out to help us be eyes wide open at this critical juncture.

Thank you for your great presentation today. It has been thought-provoking.

Rebecca Hines: Indeed. Maya, do you want to bring us back home before break?

Maya Bernstein: Yesterday we had a presentation by CMS and ONC about the new interoperability rules, and they are promoting the idea that we should be able to use an app to get access to our own data, which everybody I think supports the idea that people should have access to their own data. However, I'm wondering who is making those apps.

Are you suggesting to us that the Chinese are making those apps and we're going to download Easy Health 1,2,3 to get access to our data and we may not know who is behind that app and that is a way for the Chinese to be collecting data on us? Or are there other things related to those rules that we should be concerned about?

Ed You: I would consider that a given, that it should be part of the risk assessment. Look at what's happening in the news, like TikTok or being affiliated with China. That app is wildly popular among the young generation. And there was that other app that can age your picture, your photo of your face, and that turned out to be a Russian entity as well. So, yes, absolutely, it is a target of opportunity.

It is not just a privacy issue but it's looking at now data is a commodity, bottom line, and we need to start looking at it from a security lens in that aspect.

Maya Bernstein: That is interesting. The problem that I see is that when we talk about doing a risk assessment, the emphasis that yesterday we heard from CMS and ONC is that we are going to do

consumer education. We are going to make sure that the agreement that you sign when you sign up for an app is something that consumers can understand and so forth.

My experience with those is they are 10,000 words long and multiple pages, and there is no regulation that requires any of that. So I'm concerned that we are putting a lot of burden on individual consumers who don't -- I don't want to be paternalist, but most consumers who are going to have access to this stuff are probably not going to have -- I mean, look, I don't read that stuff, and I do this stuff for a living. How many of us actually -- ? Occasionally I do. When I go to my doctor's office, I scratch out what I don't want. If it says I'm going to give my data to research I say no, thank you. But most people don't do that or don't even know that you could do that.

It seems to me we're putting a huge burden on the consumer population which is not equipped to actually make the kinds of decisions that you're talking about us having to make.

Ed You: Right. And that goes back to how do we raise the level of awareness and discourse as quickly as possible. It can't just be on the consumer. It has to be some element -- again, as I said, it's a whole-of-government, whole-of-private sector, whole-of-academia issue, so there has got to be a trickle-down as well as a bottom-up grass roots approach and understanding of this as well.

Maybe this is divulging too much personal information, but on the bioeconomy front, I have been at this for coming on to five years now and it wasn't until the last couple of years, where it finally started gaining traction. And I hate to say it, but the COVID19 pandemic really brought to light some of our dependencies or vulnerabilities on a foreign supply chain.

I am hoping that when we do get through this, there are going to be some potential, very plain ways forward to look at that. And I'm hoping that this aspect of bioeconomy is addressed as well, too. I have a feeling that there will be a window of opportunity.

But you're right. It can't just be on the consumer. If anything else, if that is the case, then we had better put out some robust education materials for them.

Rebecca Hines: Maya, the scope of this committee, for the committee to reflect on, is there some way in its role, in its bully-pulpit, to encourage strategic thinking like this at all these different sectors you have outlined? I think that might be something the subcommittee wants to look at, because you said a few minutes ago that people are taking the short view. They're looking at profit, short-term investment, and that is the driver for how we got to where we are.

The People's Republic of China is taking the long view, and they are making all these strategic investments. And so if we want to really get into a new way of approaching security we have got to take a strategic approach.

So, if the committee could, for instance, recommend something along those lines of -- obviously, our recommendations go to the Secretary of HHS, but our reports are widely read. So it seems to me, after our break we need to talk about what is the role of the committee potentially in encouraging this kind of strategic grasp and really disseminate the need for strategic thinking and investment in a way that hasn't happened.

Ed You: That would be phenomenal. If the committee is willing to do that, both from a personal as well as a programmatic standpoint, that would mean a heck of a lot.

Rebecca Hines: We cannot thank you enough for elucidating the issue of security in a way that I certainly haven't heard and it sounds like many of the members haven't heard. If you have nothing else to do, you are welcome to rejoin us after the break. My sense is you are probably a very busy person.

We are going to take a 15-minute break and will reconvene at 11:20. And remember to mute yourself while you are on break.

Thank you, Ed.

Break

Rebecca Hines: We are back from break. Frank.

Subcommittee on Privacy, Confidentiality and Security

Frank Pasquale: Thanks so much, Rebecca. This is going to be our discussion of project-scoping with the Subcommittee on Privacy, Confidentiality and Security for 2020 to 2021. We have been in discussions on this work plan in the spring. We have new members and we are really thrilled to have new members onboard. The existing subcommittee has had long-term discussions of many issues about what should be in our work plan.

Just to go through our rough estimate of time, you can see we are a little off time. This is just put up to give you a sense of general issues that we will be dividing up for the discussion.

For about the next 15 minutes I will give a sense of some possible areas of focus that have emerged out of the subcommittee's discussions. We will also talk about the scope of the problem for another 10 minutes or so. Then I really want it to be an open committee discussion because I think what's really important for us is ensuring that the subcommittee, in terms of its future work, has buy-in from the entire committee. And finally, we will talk about some next steps.

In terms of our PCS focus for 2020-21, here is sort of a broad overview of the types of issues that we have been discussing in calls and emails. First is something that was not something we were thinking about until this month, but given the unprecedented epochal nature of the COVID19 challenge we really wanted to be able to talk about building a trusted public health surveillance infrastructure in the face of new pandemic threats. We exchanged some information about that, particularly from across a national perspective because we think that there is a lot to be learned from countries that have flattened the curve or have otherwise been addressing the issue.

Also, there is an emergent and I think very urgent discussion about emergency authorities, and we have some expertise on the subcommittee, particularly with respect to emergency authorities, so we wanted to potentially have some discussion there and some focus there. So that is one potential area of focus.

Another, which is something that has been consuming our attention for some time and that we have also developed expertise on, is unexpected or unintended consequences of interoperability rules requiring HIPAA-covered providers to transfer data to non-HIPAA covered entities. We got a good sense yesterday from two excellent presentations in that vein with respect to how some of these issues might come up.

I raised the question yesterday with respect to potential transfers to foreign entities and choice of law rules, to what extent would the US law apply to that or would other areas' law apply. Are terms of service the key there? Are there ways to deal with the possibility that terms of service might be inadequate or inadequately protective?

So those are just a few of the things that we could talk about in that area and could focus on. And I will be sure to mention those as well, and I will be developing all of these points later on in the presentation.

The secondary topics are topics that have come up in our conversations but that, in the interest of time, I don't want to delve into too deeply here but that certainly we can go back to. Some secondary topics would be artificial intelligence and data. That is something that's becoming an increasing area of focus. With respect to AI and data, is the data representative, is there bias, are all affected groups in society adequately being addressed? That I think is really critical.

Another is the data on opioid and substance use disorder is something that's an ongoing concern for many agencies, for those are trying to care for those suffering from opioid and substance use disorder. Part 2 was mentioned, so that's something that has been out there as a potential area to consider.

Standards for terms of service of health apps. Just following up on our work on non-HIPAA covered entities, one thing we might be concerned about is are there standards for terms of service when data that is coming from a HIPAA-covered entity goes to an entity that is not HIPAA-covered. Particularly, we know that, of course, if that is done directly it is covered by business associate agreements, but if it's done indirectly, for example, at the behest of a patient or going through a patient's app then on to others, then that chain might be broken, that chain that was anticipated in the high tech app, and there's a little concern about that.

And then finally, a research agenda on de-identification methods and how technical expertise may be necessary there.

Now, because it is one of the primary topics, Topic A, I wanted to go through six aspects of the scope of trusted public health surveillance infrastructure and as a topic of concern and focus for the PCS work plan.

The first would be on technology, the actual and potential affordances of technology. Second, clarifying emergency exceptions to extant rules regarding data collection, analysis and use. We have already seen some very important efforts there to inform the public of these emergency exceptions, and inform providers, of course. Then the question becomes to what extent do we want to clarify the scope of those, the duration of those, what happens to data after it is collected.

Third is secondary uses of data that might be collected in the midst of a public health emergency or via novel authorities that are generated in, say, pandemic preparedness.

Fourth, ethics and bias. Are there ways in which the data could be used in troubling ways? Are there ways to anticipate that to try to minimize bias problems or ethical problems?

Fifth, security. We have heard a lot from Ed today about security of data, and we also got very interesting insights from the Cybersecurity Framework from NIST. And are there ways of ensuring that these types of concerns are not going to be imported into our ongoing data collection efforts -- not our ongoing data collection efforts, but to data collection efforts overall.

And then finally, the patchwork-of-laws problem which I think is something that is of some concern to providers, even given OCR emergency guidance.

In terms of looking at technology's actual and potential affordances, in terms of international examples there are a lot of ways in which countries are trying to deal with this novel problem. If you look, for example, at Singapore there is an app called TraceTogether, and the government asks that individuals use this app that uses Bluetooth contacts to try to give authorities a better sense of who might have been in contact with COVID19 carriers or sufferers. That I think is an interesting example of very rapid deployment at scale of novel forms of public health surveillance.

Taiwan has also used location data from telephone services or telecom services. There was a widely reported story yesterday of someone who was supposed to be in quarantine for 14 days. They did keep their phone charged all the time, and 15 minutes after their phone ran out of power and was no longer pinging the telecom providers as to their location, they were visited by authorities to ensure that they were actually in quarantine as opposed to breaking quarantine.

China has partnered with a financial firm, Alipay, to give people an app that would use data to report on health status. Green would allow one to go out, red would be a requirement for quarantine. There is already some initial criticism of this because the data involved was not transparent, so people didn't know exactly where the data was coming from or how those determinations were being made.

Israel has already seen jurisprudence on this matter. The Israeli government ordered that the national security data be annexed to public health monitoring. I believe -- I haven't read this case yet; I'm still looking for the case itself, an English translation of the case.

But the bottom line of the supreme court intervention there was that the relevant parliamentary committee was not involved and so there was some concern by the judiciary that there was not adequate executive supervision of this type of data. And finally, the European data protection supervisor has gone in the direction that I think our OCR has gone in terms of emphasizing the flexibilities and ability of any of these to gather relevant data that they would need.

The domestic proposals, Part B, that have been reported at least in the media, although I have not seen language on these yet, address telecom data, extant corporate data and special app data that might be used in terms of trying to ensure that there is a more robust infrastructure for potential contract-tracing or other interventions that might be necessary either now or later in second or third waves of the virus.

I want to note that, in terms of emergency exceptions, we have already heard in terms of some emergency guidance by OCR with respect to imminent threats and flexibilities that are given to entities when they feel that there is an imminent threat. But one of the issues here is that stakeholders may desire more clarity in advance with respect to the scope of those exceptions, the scope of, say, non-penalties. We have heard of that in the telehealth area already, but we may get some demands in other areas. Moreover, what I think is critical is the need for guidance after the emergency with respect to the use or disposal of data collected or shared during the emergency.

So there may be very large affordances given to entities to make novel collection, analysis and use, but then what happens afterward? I think that is unfortunate because we have had many examples of emergencies in the past -- for example, Katrina and other areas -- but I think it's something that we finally need to address in terms of giving after-emergency guidance.

With respect to Theme 3 of Topic A, secondary data uses, several privacy advocates have argued that the data gathered via novel monitoring and surveillance infrastructure should only be used for public health purposes and/or deleted once the emergency is over. But advocates for research may wish to secondarily use these data for research. I think there is a really robust discussion to be had about the range of secondary uses that would be permitted or forbidden in this area.

With respect to bias and ethics, one concern is also selective use of data. It is hard to build a trusted public health surveillance infrastructure if it is only, say, certain communities that are being affected by it or being controlled by it. And so I think that is sort of an issue that comes up. I have already mentioned the Alipay Health Code from Ant Financial having a lack of transparency as to where it is getting its data from.

Paul Ohm, law professor at Georgetown, did a critique of Google Flu Trends. Google Flu Trends was initially hailed as something that would be quite useful to authorities in terms of early warning signs about potential hotspots of flu and other respiration illnesses, but there are some valid concerns about using big data as an information tool in public health infrastructure if there isn't adequate ability for individuals to scrutinize the foundations or bases of these.

And premature release of improperly anonymized data, there have already been some complaints about South Korean footpath data. Apparently, some entities were very zealous about avoiding a reprise of what happened with the person called Patient 31 in South Korea. There were 30 patients who very successfully self-isolated, but Patient 31 almost started an uncontrolled outbreak by defying the quarantine regulations and going to a salon, going to church, doing other things.

There was a concern there, and so there was a release of some footpath data, but then some individuals ended up being harassed, or at least that was the concern that I have seen reported with respect to that.

So there are some potential solutions with respect to, say, apps such as the Singapore app, TraceTogether, which is based on Bluetooth and location data, that it might be more privacy protective. And there is an AI ethics literature on representative and fair datasets. Sensitive data and database interoperability may require higher standards of security as well.

The final theme of Topic A is the patchwork approach. The patchwork approach concern is that, even though there are emergency authorizations with respect to HIPAA to share data in the face of imminent threats, there are still lawful use requirements that refer to state laws that might be seen by some providers and by some public health authorities as impediments to the sharing of data. In terms of thinking about that and the viability of the patchwork approach in light of new pandemic threats, I think there is a lot of re-weighing of the balance of say federalism or federalistic approaches now, and that might be something that would be a theme within this public health surveillance infrastructure as well.

Now we are on to Topic B, looking at Beyond HIPAA and thinking about the potential unexpected interactions of the interoperability rule with some of our Beyond HIPAA concerns.

Just to review, we know that there are HIPAA-covered entities and then there are all other data users and data holders, and we realize that there are mechanisms, both public and private, to ensure that data is transferred in a responsible and equitable way. But there still is lingering concern that essentially the HIPAA protections are pretty robust, particularly, as I mentioned earlier, that idea of the chain from

the covered entity to business associates to subcontractors. And the concern I think when we go beyond HIPAA is lacking that chain.

The other concern that I think comes up in the context of the consumer education strategy that was mentioned yesterday in terms of dealing with new patients' abilities or technological approaches to access is concern that consumers/patients may not understand that HIPAA doesn't apply to the non-HIPAA covered entities that they might transfer data to.

The concern here is that, based on our work, our already published work and work that has been shared in many contexts with respect to Beyond HIPAA, there might be cause to revisit those recommendations with respect to new risks that are on the horizon based on new affordances to share information with non-HIPAA covered entities.

That I think is one thing that is part of this topic and it's something that is already under consideration I think in many jurisdictions about the spread of health data to, say, potentially unvetted apps or apps that are governed by laws that are not US laws, or apps that have terms of service that provide for protections that are far short of what someone would expect in the health context. I think all of those are clear and present dangers with respect to health privacy, confidentiality and security, and they are something that would be another area of focus.

The suggestions that I would bring forward in this presentation are that a primary focus would be a trusted public health surveillance infrastructure in the face of new pandemic threats, looking at least some of those six themes that were mentioned earlier in the presentation. And a secondary focus on the unexpected or unintended consequences of interoperability rules requiring the HIPAA-covered providers to transfer data to non-HIPAA covered entities. I think that both of these focuses are really topical. I think they would require an environmental scan to start with, especially the first, because we are just beginning to deal with this first problem at least with respect to the COVID19 context.

But I would also want to do the environmental scan with the secondary one. We already have a good existing dataset with respect to comments on the interoperability rule, some very insightful comments that were concerned about exactly this type of topic.

With that, I have gone a little over with respect to the anticipated slides and presentation. I thank you for your patience. I think it would be great to have a discussion now and I will be sure to be taking notes, and I know that Rebecca is as well. Thank you.

I see first on my screen Vickie Mays and then Lee Cornelius.

Vickie Mays: Thank you. I guess I want to focus on two things. One is the public health surveillance, and I think we may want to think about how much. I can imagine in a scoping document what we have to think about is how much of that to cover, because I think there are several parts to it. There is the part of public health surveillance that has to do with just epidemics and what do we do about data in general. There is public health surveillance that I think is really about the space in healthcare and population health.

So I think public health surveillance is really big, and I am going to hope that in this discussion we can have some sub-topics under public health surveillance and then come up with a priority of what it is that we want to look at.

The other side to this we haven't talked about much and that is the notion of either our duties or responsibilities when it comes to the protection of research subjects. I think that becomes important relative to public health surveillance as well, and that to me is almost a different path than the other, but I think it is a very important path and the presentation today helped underscore that.

So I just want to see us probably morph into, if we pick public health surveillance, really trying to get some buckets underneath it and figure out how to prioritize it so that we can get a good scoping document.

Frank Pasquale: Great, thank you. I completely agree and I was taking some notes and I think that is a really good perspective. Lee?

Lee Cornelius: My reflection as I sift through a lot of our conversations here today, is I would use the word dynamic in terms of the charge moving forward. The reason I use the word dynamic is that, with our discussions and exposure to issues about acknowledging the bioeconomy, artificial intelligence, I worry about -- I mean, I love the conceptual frameworks, I am very much a fan of strategic long-term planning. I get that. That is the charge of the committee.

At the same time, we have to figure out how to interweave this through our regular cycles of deliberations to where we are always on top of the fact that the knowledge base and the applications are moving very fast, and the ways that it will influence privacy and security are going to be different, let's say, six months from now and nine months from now.

I don't have the answer for that, but yet, I think the key is dynamic and our thinking being both nimble and strategic.

Frank Pasquale: Thank you. I completely agree. I think it is a very delicate balance. I forgot, but I meant to start the presentation on exactly those lines in terms of saying that it is a hard balance because we want to be relevant but we don't want to just go after every shiny new object.

I do feel confident that the COVID issue is something that's going to be incredibly important for at least a year. But I appreciate that and thinking about how to balance the relevance versus our timeframe and our rhythm is critical here.

Nick Coussoule: I actually like both of the topics. The one question -- and I guess this is posed to you and the other committee members as well -- is what else do we know might be happening across the industry in each of these areas such that we would need to make sure we were addressing something that we could attack but also wasn't being duplicative and maybe even being leveraged.

Any insight into whether these things are being looked at by other entities or groups?

Frank Pasquale: I think part of the environmental scan would definitely be trying to ensure that we are looking at what the frameworks were from industry partners. I know in my experience there are probably 300 to 400 AI ethics frameworks out there nowadays. Nature just did a meta-study of all artificial intelligence ethics frameworks including industry, government, civil society, et cetera. We probably don't have the bandwidth or resources for that, but we can at least go to some of the major players and see how they are trying to address these issues.

Yes, I think that is going to be the first step. A very important first step is ensuring that we get this overarching view and not duplicative.

Vickie Mays: This is just a follow-up to the question that was asked by Nick. There's a lot of work in the AI space, so to some extent, if we had to let something go -- I am really big on AI but there are a lot of people in that space and we would have to figure out exactly where to land, and I think there are some other things that we probably can do and do better.

Frank Pasquale: I am in total agreement with you there. I think that is a good way to narrow things down.

Rich Landen: I want to build on Nick's comment and take it a step in another direction. I think besides our own landscape survey or whatever it is, finding out who is doing what, we need to think potentially about, like we are currently doing with ICAD, who do we partner with who has the expertise in the areas that we don't. I'm thinking back to the FBI presentation today. There are just aspects of this that are mostly outside the scope of our resources.

So, whatever we wind up doing, can we do it by ourselves or do we have to partner with somebody who has expertise in the areas that we don't?

Frank Pasquale: Yes. I think that is a really good idea in terms of thinking about potential partners in this area. I do see that is a trend in our committee overall, is trying to get more work -- I think that does leverage the impact and it does also help cover areas that we may not necessarily have the depth in. Thank you. That is something we will definitely go back and consider.

Bill Stead: I haven't seen any other hands and I will just weigh in. I think that this area almost has to be first, given what is going on. And I do think if the early part of an environmental scan could have the two threads that have come up from this conversation -- one, how do we find the scope of public health surveillance -- I think that is the right short name. It would sort of be a touchstone as you have what is in and out based on that.

Second is who are potential real operating unit partners. In the work we did on the community health and wellbeing measurement framework, having the strong partnership with Karen DeSalvo and Denise Coo, who was assigned to her, at that time gave us, you know, people who were operators to help work with us. And the other clear example is the way the NLM helped us with terminology and vocabulary.

So I think if we could build a short list of who those potential partners were, as you define scope, that would probably give you what you need to move forward.

Frank Pasquale: Great. I think those are very good suggestions. I really appreciate that.

Denise Love: I really like where you are going with this, and I just don't have a lot to add except, as we look at partners, sometimes I feel we need to look hard at the state level epidemiology and public databases. A lot of the conversations around this area not only touch on de-identification and the work that states have put in there, but there is real concern about downstream use of surveillance databases, what is proper, what is not. There has been expressed concerns that some of the private databases have less of their hands tied for use than government databases, so there seems to be some disparity in how those downstream uses are looked at, if at all.

Frank Pasquale: I agree. It's a very interesting problem, and it is one where, if not parity there, at least some attention to the disparities would be really helpful.

Alix Goss: I want to build on what Denise is talking about with the public health database aspect and build upon that from a perspective of the interoperability objectives that we have heard from ONC and CMS, but also to think about a trusted exchange framework within the United States that's going to start to bring a new flavor of opportunity for privacy awareness and may also provide us with an opportunity to tap into the numerous procurement-related references to help the states understand some of the implications of their business decisions. Although they don't anticipate permitting any US content going overseas, there are still aspects of state procurements that tap into healthcare services and supports.

And so I think if we can have a multi-layered approach to stewardship rules that gets refreshed and then trickled out to the various segments of the healthcare population and administrative and state government processes to tie it all together, that would be helpful. Because as I have listened to the earlier presentation and then the focus areas, I felt like this issue is just steamrolling down a hill and may get ahead of us unless we can pull it back and start to segment it in the projects like the environmental scan aspect.

But also there is this longstanding body of work within the full committee related to vital records and that very fragile ecosystem and infrastructure that is now being tested even more, and if we can provide data stewardship and guidance to help them, that would be awesome.

Rebecca Hines: Alix, this is Rebecca. I don't think I captured the main point you were making, and I apologize. Can you sum it up for me?

Alix Goss: It was very multifaceted thinking. The point is that we have activities in the federal government and state government that we need to think about as our projects emerge. I think grounding it in an environmental scan is important. But I think we have got to be mindful about our historical work not just in PCS but also in population health, specifically, vital records and public health infrastructure.

Frank Pasquale: Great. Thank you. I think that is a really helpful multidimensional frame here. Thanks. Bill?

Bill Stead: Let's let Melissa Goldstein go first and then come back to me.

Melissa Goldstein: This dovetails a little bit with what Alix was saying. This is the first time that the new federal CDC regulations have been tested, essentially. The regulations mostly focus on quarantine, but there is data production, data analysis, data collection that is all part of that. The country's very first actions were in California, and what do we do with the people coming back from China, and the data and how is it separated and how is it used. It strikes me that we need to focus on both the federal government and the states in terms of reporting, when they reported, how they reported.

And of course, it all is mixed up with the testing availability. So it's going to make a difference in when we have the data, when the public health surveillance structure have the data and what happens to the data. And as this all shakes out we will hear more and more about privacy issues. They are starting to trickle now in the news, but it is only a trickle now. But when things calm down and people are less scared, honestly, I think we will hear more about it.

I think it's great to start with the environmental scan because then we will know more about what people are actually thinking about the surveillance infrastructure in general, both from within public health and patients in general, consumers.

Frank Pasquale: Great. Thank you. I think that's a really nice way of framing it, Melissa, because I think that will sort of stage things much better.

Bill Stead: Thank you. I think one of the key dividing lines that might help us frame opportunities -- most of our historic thinking about public health reporting and data has been individually identified data, and our statistical practices have involved in essence aggregating it into large enough groups that you could not identify people, but it's still basically data that builds from identified data.

The Bluetooth example is an example of data that is in essence able to identify where contact is occurring. It doesn't necessarily have to be identified.

So I think if we are going to think about a public health surveillance system at scale, one opportunity that we should explore is to what degree can it be with what is very close to synthetic data, if not synthetic data, even though it's derived in real time from real things people are doing but it is not moving around identified packets. I think there are probably two directions over time that would need to work together. One is getting the right robust vitals and related data infrastructure that is, in fact, identified and having it collected and maintained in a scalable, secure, privacy enhanced fashion.

The other is really getting good at using non-identified signal of patterns in the population that may tell us we have got to turn on identified data in an area, but then we're going in and doing it in a very targeted way, informed if you will by that other pattern. So that could be a way to think about how this might work out over time.

Frank Pasquale: I really like that, Bill. I think that is a really nice way. I think part of the environmental scan and part of the eventual report will be thinking very clearly about sequencing different types of interventions, and that helps a lot in terms of thinking about the steps between de-identified and identifiable data uses. Vickie?

Vickie Mays: I would suggest one of the things we want to think about for the non-governmental, non-state types of data that we also should focus on. It is interesting because that was one of the questions to us by Sharon when she said can you think of any datasets or data that we could be using, and I know right now in California there is lots of activity going on in terms of social media and there are a lot of different things that are being tapped into to figure out -- like, for example, one of the things that's being used is Nextdoor.com. I don't know if you all have it where you are, but they are looking at discussions of who needs what, what kinds of things are going on, as a way also to try and find out where vulnerable populations might need information for testing. The mayor's office, for example, is tapping into that.

So there's a lot of other things that it's very interesting if we think creatively about and will give us indicators where individuals who might not be calling the Department of Public Health but are asking publicly for help could be identified. That is one point.

The second is I think we need to also consider international issues here. For California, we had a ship that was sitting, and part of the politics really was about who owned what, who could do what, whether

or not those numbers on the ship were going to become California numbers, would it suddenly for us look like we were a hot place, that we had already reached where New York was.

So I think we want to think about whether we want partnerships with WHO or PAHO or the National Academy of Medicine, because there are some very interesting data issues that are beyond just us and the states, and the rules that govern claims and everything else are going to be important for us to examine.

Frank Pasquale: I really like both those ideas, because I think those novel data sources are increasingly -- I'm looking at the partnership between, for example, Amazon Ring and local police departments. It is remarkable to look at the degree of integration of private and public infrastructure there that has happened very rapidly. I think similarly the NextDoor data will be incredibly useful but also something that we want to be sure to have a handle on all the privacy and security implications of that. Jackie?

Jacki Monson: I echo Vickie's comments. There are a lot of interesting data points. Just something as simple as Lyft, they're tracking geocoding of patient information. You know, if you have a patient who you're trying to get to an appointment and you want to know how soon they are going to be there, they're tracking geocodes for that. So there are a lot of areas.

The other area I think we need to think about, knowing that I am sort of in the crux of this with, in the last week and a half, over 105 data requests from Sutter's data - we have around three million patients and everybody wants our data right now, particularly related to the crisis that's going on because many of the patients that came from the cruise ship and other places have populated Sutter's hospitals.

The interesting piece in the analysis is it's all coming from what I would call intermediaries, so third parties. For example, I think we talked a little bit last week on the committee about EPIC and what is an electronic health record's role in this, and should they really have the absolute right to just pull data because they have access to EPIC. So, for the rest of the committee who didn't participate in our call last week, the request came from EPIC to all of the CEOs of every single hospital that EPIC is in that they have 24 hours to opt out, and if they don't opt out they are going to pull all their COVID19 data including not just de-identified by identifiable data as it relates to those patients and provide it to CDC.

And so, obviously, when I get something like that, that is kind of alarming, and I am not sure that we contemplated that as an industry as much as we probably should and perhaps have guidance around what is the role of those third parties with respect to the data. And really, should they be in the middle of that, because as healthcare organizations we also have obligations to tell our patients how their data is being used, particularly in California.

So I think there are just a number of issues around this. I think it's an important area and there's just lots to contemplate.

Frank Pasquale: Thank you, Jacki. I think that is really true. I think the type of things that you are describing are very important to get a handle on, and there is no lack of really difficult issues. Denise?

Denise Love: I am sorry I got called away for a call and this may have been emphasized. I like everything I have heard. We talked about novel data sources that Vickie mentioned, but what I'm seeing is the novel combination of existing public health surveillance and novel data sources.

I saw one display of taking suicide and mental health diagnoses and then geo-mapping mental health centers versus gun stores and finding out that gun stores are much more prevalent in those zip codes than the mental health centers. But overlaying a whole lot of these datasets together is really kind of challenging our views of de-identification as well, if that is even a word. Maybe rename de-identification to something else.

Another part of public health surveillance that haunts me and haunts the people collecting surveillance databases is the payer and provider redactions for sensitive information, either those required by law or perceived law, and it's quite erratic and it really puts holes into our surveillance system, especially when we are trying to look at an emergent condition.

Frank Pasquale: Thank you. That is a terrific addition. That is not something I was thinking about, but it was something -- I actually convened a panel once about fuzzing data sources and the way that made it more difficult to find particular niches in demographic groups, and I think we could definitely plug in that current concern to some stuff that has been written about, some critiques of the fuzzing of data sources, ways of removing sensitive data.

Alix Goss: Frank, I want to build on the comments from Jacki Monson and link it back to sort of the environmental scan discussion. We talked about partnering to really baseline ourselves, but I am also thinking that in addition to doing that environmental scan there might be a good opportunity to convene a roundtable in early federal fiscal year next year to take a deeper dive into this.

I think we have had tremendous industry engagement over the years, but we are at a new point. We are looking at things through a new lens, as Jacki pointed out, and I think that the engagement of NCVHS with industry is a hallmark and it also ensures that we are on firm footing, and that we also then have an ability to spread the word related to the consensus-building that we do and the byproducts that come out of the multi-faceted efforts that we undertake.

Frank Pasquale: Yes, agreed. I like the idea of a roundtable because I think inviting in all of the stakeholders and getting the industry perspective is critical.

Alix Goss: I think you can do it as a part of the environmental scan effort. We have done this in a variety of ways just as a process that we can undertake, but I don't want to be just bound by our past, but we do have some best practices that we can carry forward.

Frank Pasquale: I don't see any other hands right now. Is there anybody else who wanted to weigh in or have other perspectives?

Rebecca Hines: Frank, if that is not the case, then I think what we need to do now is, based on what Alix just said, it sounds like we have some broad outlines of what would feed into a project scope document.

Frank Pasquale: Yes. Definitely.

Rebecca Hines: It sounds like it is the public health surveillance and data source issue, I think the way Bill framed it, perhaps.

Frank Pasquale: Yes. I think that is a really good frame there, and I think that really does help to focus. I realize that having six themes, that was pretty broad, and I think the bullet points that you're showing now from Bill do help to focus attention there.

I notice that Maya and Bill have their hands up.

Bill Stead: I am totally in agreement with what has just been said. I didn't know if you wanted to make this the one thing you were going to try to narrow down and do, which is bigger than a breadbox and will keep you out of mischief for some time and, therefore, that would be fine.

I couldn't tell from the way you were framing your recommendation whether you were thinking of also having, at least within the subcommittee, a track on monitoring for untoward consequences of the interoperability rules. That might be something that you were working that was more of a monitoring and having periodic reports possibly at full committee meetings to just sort of track that. Sometimes we focus most of our energy on one thing but there are other things we monitor with a certain amount of our bandwidth. I didn't know if you wanted to discuss that or not.

Frank Pasquale: I am up for that. I think that actually would be -- I think what I particularly like about that is we could be in monitoring mode and be able to report to the full committee as these concerns manifest. Right now, some of the concerns are hypothetical. I do think there are real, deep concerns, particularly given extant critiques of data transfers on the Internet of Things and other areas. But I like maintaining that as a secondary concern of the subcommittee with the idea that at least some of us would be looking at that issue.

Maya.

Maya Bernstein: Very interesting conversation. You have laid out several different topics for the committee, and I think it is very tempting to want to look at the surveillance. It is very much on everyone's minds and current experience right now.

We may need new kinds of surveillance in some kind of limited defined time during the pendency of a public health emergency, for example. I don't think we have HIPAA concerns, right? HIPAA doesn't need anything to go to public health. There's a huge public health exception and that's fine for covered entities and so forth.

I think for the non-covered side, we might be seeing more commercial kinds of surveillance or commercial opportunity or industry opportunity for creating new ways of surveillance that are not regulated. That might be an area that we could focus on, something more limited than the whole pandemic. Defining what are the standards or what is appropriate during these times, some kind of do's and don'ts, some kind of rules about how long to keep data, under what circumstances it is appropriate to keep data for the evaluations and research that people are definitely going to want to do. I don't want to cut that off because that is an important aspect -- research and of the work we do at HHS and other places. But just have some kind of thoughtful data destruction rule and to take those kinds of things into account.

I think there could be some room for a discussion or some work there by (inaudible).

On the AI stuff, it is very interesting, but I said in our small group meeting there is a lot of working going on around that now and there are a lot of other entities that might be taking that up. And given that, I tend to prefer that the committee focus on things that are particular to the Secretary where fewer people are looking at it and where the expertise can most usefully be applied.

Again, like on the de-identification stuff, some people talked about need to be updated, but we sort of relatively recently in the committee addressed it, and I'm not sure that we actually have the expertise -- a lot of the solutions are kind of "mathy".

The other one is on the recent rules, and I think that is another area which might be particularly ripe for the committee's work. As you heard from both Ed and from the presentations we had yesterday, its not that there is not an interest in doing that work at the Department, that's why it didn't make it into the rule, but it is not clear that there is current authority, it's not clear who else might be doing that, it is not clear what standards and rules could be applied.

I think there is an area there when thinking about what might happen given the interoperability rules where this committee really could make a useful contribution that is not currently being addressed or can't be addressed by the Department.

So just taking all of the topics, that is sort of my take on two places where my thinking is you might be most helpful and they are very interesting and juicy topics. I think there are a couple of things there for you to sink your teeth into.

Frank Pasquale: Yes, I agree. I think we had some really good exchanges before about some of these issues, and I think it's really important to think about how to integrate this with other efforts, definitely.

I was just wondering, Maya, with respect to the public health surveillance side of it, I think Sharon mentioned -- I asked a question during her presentation about some of the issues that I brought up now, and I think she was pretty enthusiastic about it, so I just wanted to confirm --

Maya Bernstein: Yes, and someone also mentioned about -- I don't remember now who it was in this discussion -- Sharon's call for ideas for places to look for data where we might not traditionally look for it that might be able to contribute to what we're doing now on the virus. I think she was very serious about that.

Every time somebody has a new idea for where data is coming from, we are immediately serving it up. Things that you might think are kind of out there and a little bit unusual, we don't care. We want to investigate. Obviously, we have to prioritize things, but we want to investigate any possible place where useful new, non-traditional types of data could be available.

That means also that we need to think about the sources of those data, what privacy rules apply or should apply. In the public health context, we don't apply so much privacy to the collection of the data. We think that for public health -- we generally allow lots of things to be collected.

We think that disclosure is another matter from the public health entity. When we think about collecting for public health, somebody is making a disclosure on the other side, but at least in the HIPAA context pretty much no prohibitions on disclosing for the purpose of public health to a public health entity, but if we're starting to collect data from other entities that are not providers, not covered entities, we might think about what rules, what standards, what practices, how we want to draw a scope around that and how we want to create rules or standards or suggest best practices I think is a ripe area.

But yes, Sharon was real serious about trying to think about what new sources of data we might look to. Then there will be a whole bunch of other rules and standards that we might have to think about because we're looking for new places for data.

Frank Pasquale: Yes, absolutely. Vickie, Nick and Rebecca.

Vickie Mays: I just wanted to go back and not lose two things. One is Lee's comment about being dynamic.

I am just getting a little concerned that if we get too full what will happen is we will kind of follow our standard path and then not be able to offer up something that I think is for the moment. It's almost like until we get them the environmental scan I would almost say I would put the monitoring of interoperability to the side, because I think that we may have to move faster than we are used to moving if we want to be relevant. I just think we need to keep that in mind.

The second is I would also hope that the Ed You presentation and some of those data issues and what's happening in terms of COVID19 and the ways in which anything from procurement and supplies that come in and what we need to think about in the midst of the ownership of that data also gets pulled into this.

We have a pretty big area, and I think what Maya is saying, I think we also want to be able to identify for Sharon the kinds of things that are sources of data to track as well as the sources of data to give her information on how to address the COVID19.

I don't want to see us take on a second thing but to kind of stick with this, because I think it is so rich but also very relevant.

Frank Pasquale: I hear that. That makes a lot of sense.

Maya Bernstein: Can I just really quickly respond to that? I appreciate what Vickie is saying. I agree. I think it will be very challenging to move faster than we normally move just because of the infrastructure and the resources that we have. We can only meet so many times. As Rebecca was saying yesterday, it takes more effort to actually set up one of these than it does to do an in-person meeting where we are all in the same place real time. So I appreciate those of you who are at 5:00 o'clock in the morning.

But I also think that, for better or worse, mostly worse, this is going to be with us for a while. I think we have some time to be able to respond to this virus but also to the next one, and to learn from what we're experiencing right now while the issues are particularly vivid. It will allow us to think about the kinds of questions that are arising that we want to respond to, and we should use that vividness or the fact that it's top of everyone's mind right now to capture our best thinking, our most focused thinking about how to deal with this thing.

I think even if we cannot move so much faster than we're used to it will still be relevant.

Frank Pasquale: I do agree. I think of this as an ongoing issue especially with climate change causing lots of emergencies as well. I can anticipate emergencies in that respect as well.

Nick Coussoule: Frank, thank you. I don't think it's disagree so much, as offer up a way to think about it a little bit differently. The practical reality of how we operate is not built for speed. And I am not being negative; I'm just saying structurally it is not.

Now that said, I think the issue of dealing with the public health information-gathering and dissemination is a very long-term structural problem. I will second Maya's comments a couple minutes

ago that regardless of whether we get anything done in time to impact materially the current epidemic, it is going to happen again, different circumstances, different situations, it might not be a coronavirus, it might be something else. I think that topic is still very relevant and very real.

At the same time, I think it is going to take a while to get our hands around how to frame something up with both the environmental scan of what's actually in play, the challenges, the opportunities. I would almost like to recommend a dual path of not only doing that but also focusing on the same thing, which is an immediate need in regard to the interoperability rules, the data-sharing and privacy challenges.

The reason I say that is that I think both of those efforts to do a bit of a scan and a framing may inform us that one or the other is more appropriate for us to delve into in detail, either given a partnership opportunity that's there, given other activities that are going to be going on or are going on across the ecosystem. As soon as I say that, in the back of my head I'm realizing there is a lot of work out there and there's not that many of us.

Now, we are all doing this as part of our other job, so I don't want to overwhelm us, but I do think it makes sense to think about both of them from the standpoint of how would we actually frame up a scoped activity that we could get done.

Frank Pasquale: In terms of the dual path, is your sense, Nick, that the interoperability rules fallout is more urgent because it's more amenable to feedback from us? I was just trying to understand that.

Nick Coussoule: That is a great question, Frank. I don't know that either of them is more urgent. I think they are both very real right now, but I think they also both lend themselves to very structural kinds of questions. I don't think either of them is a quick fix by any stretch of the imagination. I do think they both fit into the mantra and the charge that we have as a committee.

I struggle a little bit with exactly how to frame either of them, to be honest with you, to something that's manageable and doable. There are obviously lots of minds here that can work through that exercise and would work through that exercise regardless of whether we chose to do one or the other or eventually neither or something else. I am less concerned with that and more that I do think they are both very valid exercises for us, and I think the environmental scans may inform us and potentially even drive towards one or the other.

Frank Pasquale: Got it. Thank you. Rebecca, what time are we stopping?

Rebecca Hines: We were supposed to break one minute ago so that is one thing to be aware of. I just want to make sure that we don't lose track of the security issue that was raised in the previous presentation, and is there an opportunity for the committee -- I think what I heard, Ed, you say is that there isn't anyone right now thinking strategically about this, and is there a role for the committee to put out some kind of a message on the need for the whole industry really to just shift its thinking.

Vickie said it as well. It just seems like we have not really discussed that. Is that something that there is interest in carrying forward?

Frank Pasquale: Got it. The security side would be on the public health side or the interoperability side, or both?

Rebecca Hines: Actually, I think it would be both given all the aspects, the facets of these European companies sharing data and being a one-way street, that we are sharing data there but they are not sharing data back. That was one piece of it.

Then there's the issue of people taking into account the current situation when making pretty big decisions, like is it possible -- and he used the word sinister so I'll just quote him -- you know, that China could end up with all of the intelligence, if you will, the wherewithal to develop some key vaccines and they would prioritize their own population first over other countries' populations if they had a corner on the market.

There was a lot there, and it seemed like the role of this committee, if there was interest, wouldn't be to deal with those issues but to say there is an awareness problem, folks, that we need to think strategically, and this committee thinks there is a need to think strategically in a way that is not happening right now.

Frank Pasquale: Got it. I can totally see that.

Maya Bernstein: I was just going to respond to Rebecca's last remark quickly. I asked Ed to come because I knew that he would be provocative, which he was, and interesting and bring a new perspective. But he is still one perspective. We haven't heard from people who might disagree with his take, so I want to have some caution. Obviously, he has a lot of expertise, but he is selling his ideas and trying to get across what he has been thinking about. He is still only one idea.

So I don't want us to think about taking and running with everything he said without hearing some other perspectives on it. Look, the United States Government is doing the same thing, I think, that the Chinese are doing. If we had a vaccine we would probably prioritize our own people, too. So I don't think that is necessarily nefarious. If we had as big an outbreak as another country, we would probably treat our own people first.

I guess that's all I really had to say about that. I don't want to take up the rest of your time talking about this. I think it is important to think about those issues and that's why I asked him to come. I hope you found it provocative and interesting. It certainly generated some discussion.

But we have other issues as well that we can take up, and we can be aware of them and take them into account at the same time but I don't want us to push everything else aside for that. That wasn't the purpose of my getting him to come talk to you.

Frank Pasquale: Great. Thank you. I really appreciate that nuanced perspective. Denise?

Denise Love: This is probably working the problem that we can do down the road, but I didn't want to lose this thought, to follow up on Nick's earlier comments about how interoperability and public health surveillance and this dual track. I have long felt that public health surveillance is really the benchmarking -- it takes years to do a database development and do it right, and it is sort of our validity touchstone.

But I think interoperability provides that real-time or near-time signal and how to marry the two so they work more in tandem than they ever have before. I just wanted to record that I think that is a dual track that has some interest for me.

Frank Pasquale: Great. Thank you.

I don't want to adjourn the session myself but I'm wondering if anyone has any last thoughts. Rebecca, do you have any guidance as to next steps?

Maya Bernstein: Do you think you have what you need, Frank?

Frank Pasquale: Yes, I do. The notes that Rebecca has been taking are very helpful and I think they will really help me structure a good agenda for our next PCS meeting.

Bill Stead: Then let us adjourn for lunch.

(Break for Lunch)

Rebecca Hines: I am delighted to welcome our next two speakers, thanks to Alix Goss. She pointed us to Chris Muir and Stephen Konya, both with the Office of the National Coordinator. Chris is the Director of the Standards Division. Stephen is the Senior Innovation Strategy on the FHIR at Scale Task Force. So, without further ado, I will turn it over to you.

Update on FHIR at Scale Task Force (FAST)

Chris Muir: Thank you very much. Appreciate you inviting us to participate and having us talk about the ONC-led initiative called FAST, which is the acronym for the FHIR at Scale Task Force.

As was just stated, my name is Chris Muir, the Director for Standards at ONC. With me is Stephen Konya, ONC Senior Innovation Strategist and the ONC Lead for FAST.

I am going to lay the foundation or context for FAST and then Stephen is going to talk specifically about the project. We will allow time for questions and discussion at the end of the presentation.

So, our goal for today – or goals, I should say, are: to raise awareness of the FAST approach and the goals and accomplishments that we have obtained to date; help inform how the various FHIR collaborative efforts complement each other and how FAST's work is set apart; and also highlight how working collaboratively provides value to reach a common goal.

As you know, there are a lot of FHIR collaborative efforts taking place today. Some of those efforts include the Argonaut project, which works on general FHIR structure and also develops implementation guides for mostly provider use cases, the DA Vinci project that works on payer to provider use cases. There is also the Care Alliance that supports patients and consumers. Also, projects like Carequality, which implements some of these developments, but also provides structured governance around health information exchange. And then the FAST Initiative, the initiative that we are going to discuss today, addresses the infrastructural challenges holding back the deployment and adoptions of these individual solutions at scale.

ONC is convening a highly representative group of healthcare industry stakeholders and health IT technical experts. The group is analyzing HL7 FHIR scalability gaps and barriers and identifying solutions that will accelerate FHIR adoption at scale.

The 21st Century Cures directs ONC to focus on things such as working with the private sector to develop health IT infrastructure for nationwide exchange and also to find ways to reduce administrative and

regulatory burden, which will give providers more time to care for their patients. FAST plays an important role, as will become apparent later.

A lot of you have probably heard Secretary Azar. He has said on several occasions how important it is to have health IT successfully deployed because it underpins or is a precondition for truly transforming the healthcare system. 21st Century Cures gives us our roadmap in doing so. And Cures is really ONC's policy imperative for the next several years going forward.

So, ONC's policies and programs allow patients to play a more active role in their healthcare decisions and better manage their health. Additionally, the movement of data will drive research and innovation and also accelerate the latent period between scientific discovery and integration into clinical care. Our rulemaking will allow for the development of new health apps tailored to meet the different needs of patients and their caregivers. Our rulemaking also enhances transparency. Collectively, ONC's efforts will lead to new market entrants, more competition, and make healthcare more convenient and affordable for patients and their families.

So, in summary, FAST plays an important role in ensuring that the new API ecosystem, as envisioned by 21st Century Cures and supported by our recent rulemaking, is scalable and allows third party apps to enhance the way we share and use information in the future to meet our health improvement goals.

At this juncture, I will hand the presentation over to Stephen to talk about the specifics of the FAST Initiative.

Stephen Konya: Thanks, Chris. I certainly appreciate the high-level context. I am sure that everyone else on the call here and in this meeting are understanding that there are some big policy moves for ONC overall. 21st Century Cures is our guiding post here.

I just wanted to highlight, too, that on slide five there are some links to some great resources. Hopefully, these slides will be made available, if Greg or somebody could email them out to everyone who is registered or attending. Feel free to share them with whoever you like. None of this is confidential information. It is all public information.

Specifically, there are links to the landing page for the rule there. There are links to the strategy on reducing burden related to the usage of health IT and EHRs, as well as the Federal Health IT Strategic Plan from 2020 through 2025, where some of this is specifically addressed in that strategic plan. It is currently out for public comment. I believe public comment was extended to April 3rd. I just want to make sure everybody has a chance to review that and, if you haven't already, provide some feedback on that, as well.

All of this just really as Chris said, tips the groundwork that as we are rolling out APIs and making data more accessible through those APIs, we realize that there is going to be some challenges with deploying it at scale and to do that in the timeframes that people have to comply with over the next few years, the timeliness laid out by the 21st Century Cures Act and the new rule.

Today, what we are going to highlight is the FAST Initiative, specifically, and the role that it is going to play in trying to smooth that runway and make it easier for all of these things that are being developed through these different FHIR accelerators – I am going to cover that in more detail in a little bit – and taking away the infrastructure barriers that are there, hopefully to allow these things to scale more rapidly.

With that, let's start off with just the first slide. For those of you who have ever been part of any kind of a FAST meeting, you will know that at every level, whether public or just internal workgroups, we do share an antitrust notice for anybody who is concerned about hearing that you have a lot of for-profit, private payers and/or others two cents' involved, that there are any kind of trade secrets being shared or violations of antitrust laws. Please know that we go over this notice at the beginning of every single meeting. Make sure that all members understand they are not to talk about IP related issues and that they have to stay clear and be in compliance with all federal and state antitrust laws.

So, a history. Some of you may have heard of FAST in the past being referred to as the P2 FHIR Task Force. This is really from its early genesis being aligned more closely with the Da Vinci effort that was launched. I am sure many of you have heard of HL7 Da Vinci Project. That project is more focused on payer to provider data sharing in the effort of achieving value-based care.

What happened was, just as a little history lesson, the Da Vinci group at the same time realized that, hey, while we are working on creating these implementation guides on these specific use cases for value-based care data sharing opportunities between payers and providers, we know that we need to address these scalability challenges through a separate effort that is a little bit more transparent and convened by a neutral party like ONC. Many of those same individuals came to ONC and asked if we would be able to play a role as a convener and a neutral party to help them bring all of these general stakeholders together to start addressing some of the scalability challenges.

ONC agreed to that. As we started to work to identify the challenges with scalability between payers and providers, which is the P2 in the P2 FHIR task force, in that first year, we realized that really what we were focused on weren't specifically payer and provider problems, but really FHIR scalability problems, in general. So, we needed to shift the name of the task force to being agnostic to any one stakeholder group and really focus just more on the FHIR scalability aspects. That is where the FAST logo and name came into play, which was the FHIR at Scale Task Force.

There is a lot of early work that references the payer to provider relationship because of that history. We have gone through a lot of effort to try to go back and correct some of that. Since this effort has been pretty transparent from the start, you may still find some of that early documentation that says that. Everything nowadays is really focused on scalability across all stakeholder groups, not just payers and providers.

Having said that, we also realize that the data – the clinical data that resides between payers and providers certainly is of high value. If we can solve scalability challenges between the two of them, there are a lot of others who could benefit from that, as well. We always want to make sure we are doing it right and addressing these challenges in a way that hopefully benefits all stakeholders. We are also aware of any other nuanced problems that any individual stakeholder groups may be facing.

Again, it was launched as the FAST Initiative just over a year ago in January 2019. You see that along the bottom of our timeline here. I am not going to go through every bullet point on here, but really just to let you know that is when it became FAST. We really started to hit our stride with documenting of a lot of our work in a more formal manner after that.

So, how are we organized? How do we conduct the work that we do?

Well, the FAST organization is really kind of three key layers supported by a fourth external layer. The three kind of internal – this is where you have set schedules. The early deliberations happen in these

three layers here. We have seven tiger teams, which are broken down to address primarily the main infrastructure barrier categories, as well as one that focused on ecosystem use cases and then a final one which is going to be looking at how to potentially pilot any of the work solutions that come out of this effort.

Those seven tiger teams meet individually. They each have a co-lead. We are lucky that we have Alix Goss on the call here today. She serves as one of the co-leads for one of our tiger teams, the Directory, Visioning, and Scale Tiger Team. She also serves on another committee, which I will cover here in a second.

Those tiger teams are made up of 8 to 15 members, typically, based on need. Try to have a broad diversity of stakeholder perspective involved at every level. They meet on average about once every other week and go through kind of the various work products that they are currently tasked with. That is where a lot of the early kind of ideation happens and early draft work happens.

At the next layer up, we have the Coordinating Committee. This was the initial group that came together and really provided a framework for initial charter to get things launched. This group, which is about 30 to 40 members, meets monthly and then also helps guide a lot of the work of the seven tiger teams in collaboration with our chief architects. We have two chief architects, Paul Oates with Cigna and Patrick Murta with Humana. They both serve on that Coordinating Committee, as well.

Then at the next highest level up, we have the Executive Steering Committee, which is really the leadership of any participating organization at the bottom two levels. So, this would be a VP, a C-suite representative from those organizations, who come together about four or five times a year to try to get an update on the work that is being done at the Coordinating Committee and tiger team level, provide guidance and input, and then, ultimately, be well-positioned to help embrace that within their organization, to bring it back and have that executive-level support to make sure their company or organization is going to adopt any best practices or implementation guides that are rolled out. Hopefully, that gets to the deployment aspect.

Now, those are the three kind of internal levels. On the right-hand side, you see that fourth external level. This is – you know, we have got to stay small enough and nimble enough to be able to get the work done in those internal groups. We don't want too many chefs in the kitchen. We also know it is really hard to make sure you are getting all of the industry feedback and representation and expertise when you do that. So, at various points in time, we check our work as it is being developed, early and often, with a Technical Learning Community.

Currently, we have got several hundred that are part of a listserv as signing on to be part of that Technical Learning Community. Some of them have volunteered to participate in a tiger team if and when an opening arises and if they are a good fit for it. At a minimum, they are subscribed to stay in the know, receive updates, and then sometimes through public webinars or other engagement opportunities, we are able to kind of share our work with them and get feedback on it before we finalize it.

This past fall, we did a series of webinars to share our version one of all of the solutions that were being drafted by the tiger teams. The tiger teams led those webinars. Each and every one of those webinars are archived and available where if you wanted to go back – I will provide links later – if you wanted to go back and view those webinars or see the slides from them, you could see what the first draft of those solutions looked like and the engagement that we had on that.

The tiger teams then – their next task was to take the feedback they received through those Technical Learning Community webinars and then to develop kind of a V2 of their solution, which they are getting close to finishing now.

There are a number of ways we engage with the Technical Learning Community. There is a LinkedIn group, which there is also a hyperlink in here, as well, too. Anybody can join that. I think we have got about 400 members on that LinkedIn group. I encourage as many of you and your networks to join that, as well.

The idea here is that the Technical Learning Community is a way of building awareness, providing input, making sure we are on the right track as we are going along. Ultimately, they are knowledgeable and well-positioned to take these things back and adopt them once the solutions become kind of finalized and published. So, we don't have to do a whole education campaign on the background, but rather we have a broader community of stakeholders who are in the know as we go along. They are helping build this as we go along.

Before I move on, are there any questions around the organization? I know we have a good amount of time here in this presentation. I figure maybe we could just pause there about the structure and the history. Are there any questions anybody has on that? We could also do question at the end if you want to save it for then, as well. Maybe the moderators just flag and let me know if you see any questions or hands being raised.

Rebecca Hines: Will do.

Stephen Konya: Moving on then, what are we working on specifically? What are the challenges?

If you look on the left-hand side, a lot of people get confused when they hear some people talk about FAST. They think, like, isn't that Da Vinci or I thought Argonaut was working on that. Isn't Carin doing something related to that? What about – where does CommonWell and Sequoia fit in or Carequality? We have developed this slide to try to help delineate between all of these efforts because we don't see them as being competitive in any way. If anything, we see them really as being complementary. We have had a lot of calls with all of these individual groups to try to get – and sometimes participated on panels together to help clarify for audiences where the differences lie and how they really are collaborative and complementary.

So, on the left-hand side, one thing you will see is you will see a number of organizations - there are a few others. We are working to update the slide somewhat – that are considered as a FHIR Accelerator under HL7, the top three being some of those. So, you have got the Da Vinci Project, which is focused on data exchange for value-based care between payers and providers. As Chris was talking about earlier, you have got the Argonaut Project, really looking at provider to provider data exchange as its main focus and looking at that through core data services. And then Carin Alliance, which is really focused on the consumer as their primary target. They are looking at those consumer solutions that are based on FHIR.

So, you have all of these three efforts here. There are a lot of other collaborative efforts going on. We tried to bucket a few of them below. FHIR is either central to what they are working on or maybe one component of what they are working on. The Sequoia Project obviously involved with ONC, as well, on a couple of projects. The CommonWell Health Alliance. And then you've got Carequality looking at contractual enforcement and the like.

What we see coming out of that left-hand side is really – we view it at FAST – we view those efforts as being functional use cases. What I mean by that is they are developing implementation guides or working on API – FHIR API solutions to share specific data for a specific purpose. You see the different stakeholder perspectives that they are looking at, but, ultimately, that is what it is. They are developing ways to share specific data for a specific purpose.

What we are working on in FAST is this middle category, this middle bucket. We are not saying we are the only ones working on it. We think we might be the only ones working on it across all of these categories. But what we think is that there is this gap of all of these scalability infrastructure-related challenges. This is patient and provider identify management, directory services – I don't mean directory from a sense of identifying physicians and caregivers, not a provider directory, but really more as a FHIR endpoint directory. So, how do you – when you are trying to deploy FHIR-enabled solutions at scale, how do you go out and find – in an easy way, how do you find where those FHIR endpoints reside? Right now, we don't believe really there is a solution for that - version identification and how to keep up with that, scale, exchange process/metadata, testing, conformance, and certification, and security.

The fact is that all of the different organizations involved in these efforts in the left-hand side may have a different approach to how they handle this middle category of technical areas. What FAST is trying to do is come up with solutions, to come up with common scalability approaches that include and address these barriers that are identified in the middle. The idea there is as you run these functional use cases and you try to deploy them, if we address this middle box in the right way, then you will be able to rapidly deploy and have a rapid adoption of these FHIR-based solutions in the marketplace. So, to try to really bring down that timeline it takes to run something out.

So, if Da Vinci pilots something between a hospital system and a provider system and then they roll it out to a couple other partners and then – now, you have got ten that are doing it, how long does it take for really 80 percent of the marketplace to now be adopting and using that? It could take a very long time. Part of that is because this middle category is a big barrier to doing that. They have to revisit these things every time. It kind of serves as friction when it comes to that rapid adoption. So, that is the idea.

Another way to think about it in very simple terms and we have used this from the beginning and it seems to identify with a lot of people is the cars, the buses, the trucks, the motorcycles, think of those as the functional use cases, the specific data for a specific purpose, that is being developed by Da Vinci or Argonaut or other groups. They are trying to figure out how to get it from point A to point B. They are developing that care and the payload that can go with it and so on.

The problem is the infrastructure that you see and the roadways here and how you get between those points is often very uncoordinated. It isn't standardized. It creates a lot of inefficiency in trying to share that data between different endpoints.

What we are working to do is if we do FAST right, we are hoping that the rules for the road, how cars all transmit on those roads, what are the stoplights for proceeding - think of that as your security and so on, how do we make sure that car has the access to that endpoint. You are looking at the identity issues, et cetera – that if we set those rules of the road for transmitting and we build the infrastructure in the right way, then you can have seamless, efficient infrastructure for all of these data use cases and these functional use cases to be transmitted and to get to the point that they want.

Before I move on, are there any questions about what I have covered in the last couple of slides?

Alix Goss: Stephen, this is Alix. I just wanted to note that there was a question that came in through Q&A about accessing these slides. I am assuming we will get them posted to NCVHS' meeting location as usual. I did put a link to the Confluence FAST Artifacts so that those who are on Q&A can pick that up. There is a lot of great resources that are made available through ONC's FAST Confluence page.

Stephen Konya: Alix, thank so very much. Actually, it is a great point, too. These specific slides were adjusted and tailored, updated a little bit to fit this presentation today and this audience. We do that frequently. We do have the most up-to-date version of the FAST 101 deck, which I modified for this. That is going to have all of these slides and probably other ones, as well. That is always available on our Confluence site, the link that Alix just provided. You can get lost and peruse through that site. We are always trying to figure out how to make it a little easier to navigate, but there is a lot of content on there. We really do try to be as transparent as we can with everything that is on there.

Another great resource I am going to feature later in this deck that you can also find on that site is the Annual Report for FAST. That has a ton of hyperlinks in that annual report, as well, to get you directly to some of these resources.

Thank you for pointing that out and for dropping the link in the Q&A.

I will move on. Again, if you have questions and you just didn't get a chance or you couldn't figure out how to raise your hand at the time, maybe we can unmute at the end and just log it for later.

Again, focus in on that middle box that I showed on that earlier slide between all of the different efforts. These were the technical barriers that were kind of agreed to in the early charter and then refined and ultimately published in our final kind of technical barriers document, which you can also find on our site.

So, the idea here is from a technical staff infrastructure, you have organizations, patients, users, and all of the like on one side and the same on the other side. In between that you have these technical systems that are either requesting and the other side receiving it. You can see where these different technical barriers, directory services, identity, security, testing, conformance, versioning, and scaling, where they all who up at different points and who often has to be impacted by that.

Now, the way that we are working to address these – again, I talked a little bit about this before, but this might break it down in a little bit of a clearer workflow sense. We have our seven tiger teams. They are color-coded there and happy. You can see kind of which ones are which where.

The idea is that we first work through coming up with through our ecosystem use case tiger team a number of use cases where these barriers are often felt. Out of that work, we discovered a number of core capabilities that kind of cut across all of those use cases. Those then were verified as we went back to our initially identified technical barriers and honed that document. We have a finalized technical barriers document. But each one of these kinds of support each other and all of that initial kind of discovery phase, if you will, of our work. Just making sure that we knew – had a clear definition of what the problem was and what we needed to address.

From there, if you want to click on – this is kind of a build slide. From there, we had a clear sense of what solutions we needed to focus on building. The tiger teams individually tackled those. This is the Directory Tiger Team, the Identity, Security, Exchange, and Testing Tiger Teams. Those five tiger teams all came up with solutions. Again, I mentioned earlier they had TLC webinars that are still archived from last fall. To where they said, you know, here is how we propose to address those barriers through these

solutions. We then sent that back through our Ecosystem Use Case Tiger Team. Checked them against our work to make sure that what we were drafting made sense from what the problem was that was originally identified.

Out of that work, we then took those efforts to a higher level and tried to share them with the broader team. We felt comfortable saying, okay, here is our early draft of these solutions and looked for the TLC webinars to provide additional feedback on that. And we are in the middle of setting up a number of roundtable listening sessions with subject matter experts that we are recruiting to participate and kind of check our V2 of those solutions.

Once we have got that additional layer of input, that third contribution of – you know, effort of kind of going through it, we will then look at taking those V3 – part of the exercise is to come up with an action or deployment plan that looks at do we need to combine some of those solutions into one implementation guide? Which ones need to go into a standard process that could include implementation guides? Which ones need to go through some kind of a process or best practices guide type of effort that maybe ONC could own? Which ones might need to be addressed in regulations and policy work?

At the end of that, you will see there is a dotted line there. There will need to be an effort to where potentially some of those standards might need to be backed up in regulation, as well.

After that, continue on an ongoing basis to get evaluation, feedback, to explore how to pilot these solutions, to verify them, and roll them out. The pilots also – right now, we have a Pilot Tiger Team, which is in the middle of coming up with kind of a template or a structure, if you will, of how you would be able to pilot something "at scale", which is a little bit different than a traditional pilot that we might see with standards or connect-a-thons are done today.

The idea there is once we have had this well-vetted, time-sensitive, yet cautious and methodical approach to everything to make sure we have got it right, then we figure out how do we really push hard to get the industry to adopt and operationalize all of these solutions. Again, if we are doing this right, including the TLCs, including the Executive Steering Committee from these organizations to be involved, including SMEs, nobody is surprised by the work that comes out of this. They have a good handle on our – if anything, salivating waiting for the final product so they can take it back and adopt it.

I spent a little bit of time on that one, but I think it is important to understand how we are working.

Now, I am going to focus specifically on the solutions that we have got proposed to date and that we are currently working on. These are living documents. As we go through each process, they could modify or change or new solutions could be considered or added to it. Currently, here is what we are working on.

Under the Directory, Versioning, and Scale Tiger Team – Alix, feel free to chime in at any point if you want to add some context here, since you are one of the co-leads. Currently, the challenge around directory - and this is kind of one of the primary challenges in this group – is that there are multiple places to find endpoints or in some cases no places at all to find certain endpoints, but is there a place where somebody can go to find all of them? How does that happen?

So, what they are working on right now is coming up with a national solution for FHIR endpoint discovery. Is it a federal platform? Who owns a primary platform? These are things that are being discussed and proposed and debated underneath that.

The Versions, they are looking at a way to communicate and manage multiple versions. How do we keep up with the track of that? The solution they are working on it trying to figure out how to support multiple production versions of FHIR. R4 addresses some of that, but not everybody is there or will be there in the next year or so. We know that the rule requires R4 at some point. Again, we know when it comes to managing different versions, there is still sometimes a bit of a drag.

And then this challenge of scale. How can a high volume of FHIR transactions be consistently and predictably exchanged in a hybrid exchange model? So, the solution they are working on are coming up with requirements for FHIR RESTful exchange intermediaries.

Alix, anything else you want to add to that before I move on? Don't feel like you have to. I don't want to put you on the spot.

Alix Goss: Great overview. The only thing I would indicate is that when we are referring to scale, the team has really recognized we are talking about scaling the architecture, since the entire initiative of FAST is about national scalability. So, we are starting to use the word architecture when we refer to scale.

Stephen Konya: Great point. You guys heard it straight from the source. Again, this work is continuing to evolve.

Bill Stead: Can I ask you to unpack the hybrid in hybrid exchange model?

Alix Goss: When we are talking about hybrid, we are talking about the fact that in an EHR bill, you could have an EHR to a payer direct connection, a point to point connection, or you could have a model where you have an EHR connected to an intermediary. An intermediary could be a clearinghouse, an HIE, some hub that provides it with value-added services in communicating with other entities. Just in a simple model, you could have a doctor's EHR connected to an intermediary who is connected to the payer that needs to be interacted with. On the flipside, you could also have where that payer has their own intermediary. So, you could, in essence, evolve from point to point to one intermediary in the middle to multiple intermediaries in the middle, enabling, ultimately, the provider and the payer systems to be able to exchange information using the FHIR methodologies.

Bill Stead: Thank you.

Stephen Konya: Thank you. To be clear, versions one – you know, that is where they had a good draft of all of the solutions I am going to talk about – were shared I think it was back in November. All of that is available on our site. You can look at those. You can hear them talk through the webinars that they gave. Know that there has been some changes and modifications made to those.

That V2 version, we are hoping to have a publicly shareable version of that ready here in the next 30 to 60 days. The Corona outbreak has slowed our work down a little bit and our time down a little bit here in the past month or two. We are hoping to have that posted as we take it through an S&E session. Nonetheless, you can also reach out to Alix on the Directory Tiger Team or any of the other organizations. You can reach out to us with any questions in between.

You can also pose questions like this on the LinkedIn page. So, as you are reviewing any documents or if you have had a little time to digest this and you have questions, feel free to throw things up. We want to make the LinkedIn group something that is not only just peer to organizers for interactions, but also

peer to peer. Sometimes you can throw out your ideas on there and get another peer to kind of build on that and share their thoughts on it. Feel free to use those tools in the meantime before we get V2 ready to be shared out there.

What I am covering today is largely built off of what was addressed in that V1 of the solutions.

So, under Identity, the challenge is how can a requestor and a receiver uniquely identify that patient or member? We know this is a big problem. It has been around for a while. We know that the lack of a national patient identifier is one of the problems there. How do we solve for that given the current status of things?

So, the solutions they are working on – they actually have kind of three options that they are working on. The first one that they are really focusing on as kind of an interim solution right now is kind of a mediated patient matching approach. The second being a collaborative patient matching approach. And then the third being a distributed identity management approach. I think they have even evolved this work lately to go a little bit further.

Some people have asked the question about can block chain be used. I think that might fall somewhat into the category of that third distributed identity management approach. They are also knowing that that is probably a little bit further down as far as the reality of it being available at scale. Since we are focused on doing things at scale, they need to have solutions ready in a shorter time period than potentially that might be available. Nonetheless, they are still documenting it, recognizing it. If things get there sooner than we thought, they will be positioned for that and prepared for it.

Exchange Process. The challenge is how do we enable consistent and reliable transaction exchange? The proposed solutions they are working on with that are reliable routing with metadata across intermediaries and reliable routing across intermediaries using destination specific endpoints, hopefully ones that you can identify through a national solution for a FHIR endpoint directory.

Under our Testing and Certification Tiger Team, the challenge is really how do you measure conformance to any standards that might come out around these scalability solutions? The current proposed solution is really focused on leveraging ONC's FHIR Testing and Certification Program. We have some representatives from that team that are involved in that tiger team, as well.

Security, another challenging area that continues to evolve. In this specific case, when it comes to scalability, how do we manage permissions and security across millions of patients, payers, and providers and others? The solutions that they are working on with the focus on the three areas are a trusted dynamic client registration, a tier OAuth, and then a UDAP authentication and authorization.

Again, just want to let you know the published content you see here – we have the Technical and the Regulatory Barrier documents. That is where we kind of finalize like, yes, these are the problems we are trying to address. We focused more on the technical barriers right now. We are in the process of trying to figure out how the policy and regulatory barriers come into play as we are addressing those technical barriers. We have to be a little careful at ONC in how we get involved in some of that as we shape and make some of that policy. So, we want to make sure we are doing everything per Open Meetings Act and so on and that we are following – you know, using the HITAC and other official groups for some of that, as well. We are being respectful of the process when it comes to rulemaking and things like that. We are not doing anything that we shouldn't be.

Then also you will see on the right-hand side we have got the draft solution documents for V1. There is a lot of content in those. Each one of those is several pages deep. They follow a similar format and structure. As you are reading through them, you can kind of get a sense of the layout. Those will be ultimately used in helping build and move towards an implementation guide if that is the route that that solution needs to pursue.

Again, all of that content and more is available – there is a tiny URL located at the bottom of this slide that when you get these slides you can use. It says tinyurl.com/ONC-FAST.

As I previewed earlier, we did a lot of effort to try to simplify. There are a ton of documents and content that you can spend hours and days trying to play catch-up on and going through. The best place to start if you want, I think would be to go back and access our 2019 End of Year Report. We finalized this in January. It kind of gives you both an intro and an overview of what FAST is and how it is organized, a lot of the content I covered today, a little bit more detail on the timeline and things we have achieved in the interim.

There is a ton of hyperlinks in it that drive you directly to the artifacts or the resources, the landing pages, the confluence site. Feel free to access those. I think we even hyperlinked – when you look at the other efforts that we are comparing FAST to like Da Vinci, I think even those are hyperlinked to take you directly to those sites if you are not familiar with what those organizations are doing.

I would say start there. There is a PDF version of it, as well, that you can forward to others or print out.

Also, we just put this slide in here to kind of streamline it and save you the clicks and having to go through stuff. A lot of the things I talked about today – these are hyperlinks directly to those artifacts. You can access this at any time.

For the FAST 101, we have a link to the public webinar. You will see underneath there it says FAST 101 and Keystone Presentations. That is where you will find the latest content that has been approved for us to share publicly. So, the FAST 101 and Keystone Presentations and the link that you might have accessed a month ago might be different than the one you access today because it would have the most updated graphics or content or version. We keep that as kind of a living, openly evolving URL.

The ways to get engaged in the Technical Learning Community and the link. You can click on that.

Also, we had a lot of events forecasted out for this year where we are expected to be presenting. HIMS being one of the more recent ones. As you know, many of these have moved to virtual. In some cases, we are able to transition those to being a virtual webinar instead of an in-person panel. We are still working through some of the future events and trying to figure out if we are going to either, A, still attend those, if COVID slows down and we are able to re-engage on some of those travel opportunities, or if those events are postponed or canceled or people can't make them. I think it is safe to say that in the next couple of months, everything will be probably virtual just to make things easier. Just want to let you know that, as well.

Just lastly, if you have expertise in any of these areas on the left-hand side and you want to get more involved or if you think, ultimately, you have a role to play in helping adopt and raise awareness and make others aware of the work that we are doing and get them involved, please click on the link where it says sign up and/or below that, the LinkedIn group. It is a nice passive way to kind of dip your toes in the water and start to get a sense of how we work, what we are working on, where we are at. If you

don't have the time to try to submit an application to participate on a tiger team or get involved in a more meaningful way, it is a great way to start things off. When you do have the time, feel free to reach out and say, hey, now I have got some time to get more engaged.

If you do think you want to get involved in a tiger team or a more meaningful way as of right now, when you click that sign up link, it is kind of a form you will fill out that has you explain the areas that you are interested in, why you think you would be a value to contribute to the effort, basically what is your expertise and/or experience in those areas, and then that information is shared with the tiger team leads and other leaders within the task force. They will evaluate based on whether or not they are able to kind of bring you on.

That is, essentially, the process for getting engaged. I think at a minimum it would be great to have everybody join the TLC. Certainly, looking forward, if you feel like you have a more meaningful way to contribute, just feel free to reach out to myself or anybody else involved like Alix. I know we have Lorraine Doo on this webinar, as well, who has been involved from the beginning from CMS. I know that we have others that are on this call, as well. I am trying to remember who else is on this – I know there is at least one or two others on this call that have been involved.

It is a volunteer effort. All of these people who are participating have been volunteering their time and effort and expertise. We are extremely grateful for that, especially with everything that is going on right now around the rule being rolled out and the pandemic that has been happening. We know that time is probably the most limited resource that is available in anybody's world right now. We certainly appreciate it.

With that, I think we have got just our last slide, which has I believe our contact information after the question slide. You can probably leave that one up. Feel free to open it up for any other questions that individuals might have. If you don't feel comfortable asking them on this webinar, you can always reach out to Chris, myself, or Diana, who is listed at the bottom here, as well, from ONC. We will be happy to respond as best we can. Thank you.

Rebecca Hines: Thank you so much. And Alix, thank you again, you and Lorraine both. Opening it up for questions.

Alix Goss: While we are getting the questions coming in, I just – I think Deb probably said this in her intro. Just in case I dreamt that, Deb Strickland is an integral part of the Testing and Certification Tiger Team. She has been there since the beginning. We do have – maybe that is who you were trying to think of earlier, Stephen.

Stephen Konya: Yes. Thank you. Thank you. Yes.

Alix Goss: You're welcome.

Debra Strickland: Yes. I think I did. I am not sure. I have been involved in that Certification Team, as well.

Stephen Konya: Great. Thank you. Any questions as of right now or ideas that anybody would want to share?

Rebecca Hines: I am not seeing any hands go up. Oh, there we go. Bill.

Bill Stead: I will be brave. First, thank you very much. It is very helpful and concise.

Do you have a feel for timeline in terms of when the pilots at scale would actually be launched and sort of what duration you are thinking of those so that – which would sort of give us a feel for when you might think that this could get to where you would go beyond pilots in terms of that scale?

Stephen Konya: Thank you. Great question. This is one that we have been trying to set a target deadline for – not deadline, but target date for when the activity would kick off. Our Pilots Tiger Team has been working right now to build kind of that framework or structure of like how would you actually execute and run a "scalable pilot". It is just a little bit of – you know, you have different parties that you would want to include. How would you test these infrastructure solutions and so on?

It is really – that team has been rebuilt since the beginning. So, we have got kind of a newer team. We had a bit of a start and then a stop. The newer team has been in place for at least probably about the last six months now working on that.

The target that we gave them was to look at having the draft template for how to run that pilot at scale – to have that shared internally with the Coordinating Committee here in this next month. Now, we know that with the COVID activity taking a lot of our volunteers' time in the last month or so, we have been a little more realistic and understand that might get pushed back a little bit. The idea is they are going to share that draft of that framework here in the next month or two, hopefully.

Once we get feedback and the Coordinating Committee provides a little bit of their guidance on it, they will probably come up with an updated, modified version of it. but really start to work to get prepared in the next phase. After they have got kind of an agreed upon structure of how to run this at scale, the next phase will then be beginning to recruit and look for partners to be part of that, the different stakeholders that will need to be part of that structure.

At the same time, in parallel, we are working on finalizing the solutions and potentially developing the implementation guides that would go along with those solutions. That timeline will largely dictate when the pilots eventually kick off. You will need to have that implementation guide ready to test or that solution fully developed in order for them to be able to then pilot it or test it.

It is a little bit hard to forecast that. It would be great if later this fall or by the end of the year we are in a position to start kind of setting up those pilots. We have been already thinking about what cost there might be associated with this pilot, what role would ONC play in supporting those costs, will we need members to chip in on that, can we leverage some of the other FHIR Accelerator groups to run some of those pilots or help participate in it. These are all kind of what is that data use case that we would run through that scalable pilot, so to speak. So, all of these things are still kind of in development and draft.

The short answer is not going to happen in the next six months. If we are lucky, by the end of the calendar year, we will be in a place to start piloting these things or at least setting up those pilots. Does that answer your question?

Bill Stead: Yes. It is very helpful. Given the work we are trying to do with ONC and with HITAC around convergence of the clinical and administrative data and standards, depending on which lens we have, the thing we really have to begin to wrap our heads around is if we think in chunks like three years or five years or one and a half years, when in that spectrum could we use something like this infrastructure

for something that has to run at the scale and sort of uniform nature of the HIPAA-mandated administrative transactions.

I think what at least I struggle with is how we go from the use case-based FHIR world, which has been extraordinarily successful in changing the game – how you make that to something that really has to be predictable at scale. I think this – the FAST Initiative is right at the heart of that question.

Stephen Konya: I think it certainly is - in my opinion, it certainly is something that is helping to accelerate or alleviate some of the problems with getting these use cases adopted widely and deployed widely. It will help ramp up the market.

Not having this work completed by FAST will not stop in any way current efforts that are underway from moving forward, current use case approaches that have historically been done moving forward. It will continue to dredge along at its slow pace of adoption.

Once this is ready, it will be able to kind of be dropped in a turbo boost to then accelerate and push things out even faster. Maybe it becomes something that is incorporated in the use case, the traditional use case, the implementation guide process in the future, where it becomes a consideration of like, you know, to make sure you can then scale this, you have to factor in these things or here are the best practices that we point to, here are the mandated requirements by ONC, whatever it may be. Those types of things would then be pointed to at that point.

So, it is one of those things that can be built in parallel. Whenever it does drop, it will just further complement and support any of the existing work that is going on. It won't hold back any current efforts in that way.

Another way to think about it is you can have a car – you know, we were talking about cars and buses earlier. You could have a car and right now everybody is figuring out how do we ramp up those cars, give them bigger engines, give them more payload, how do we make sure that they know where to go and so on. You can do all of that focus, but if the road they are traveling on has barriers in front of it or if it is made out of quicksand, right, cars aren't going to move very fast no matter how big of an engine you put in it.

We have to address that infrastructure. Those cars can still move. They will find workarounds. They will pull over to the side of the road and drive in the dirt. But, ultimately, they are not going to move at their peak speed or efficiency until we fix the roads. That is what we are doing now. We are trying to figure out how to fix these roads in a way that ultimately will help speed up things.

A lot of fast puns and analogies can be made there. Sorry.

Rebecca Hines: Stephen, there are a couple other questions that have come in. One is should payers trying to meet the Provider Directories Rule for 2021 follow the Argonaut model until otherwise notified?

Stephen Konya: Chris, I will certainly defer to you. If I have any other context, I can add.

Chris Muir: I will just say that is really a CMS question. We have to defer those kinds of questions to CMS.

Stephen Konya: Just one thing I was going to say, something similar or along those lines is, yes, it is CMS. I don't know if Lorraine wants to chime in here at all. One thing I did want to say about that is just to clarify a lot of that rule is specific to provider directory. There may be FHIR components to it, but it is not about, specifically, FHIR endpoints.

I know there is some language now providing to the digital endpoints, but it is – again, it is not as defined as what we might be working on. What we are working on might, if anything, build upon or complement that effort. I don't think it would be in contradiction necessarily, not if we are doing it right. We don't want to reinvent the wheel.

MS. DOO: Stephen is right. The directory that he is talking about for FAST is different than the Provider Directory that is in the CMS rule. I will just take that rule back and get – I think it came from Patrice. Is the note from her?

Rebecca Hines: No.

Lorraine Doo: It is from somebody else?

Rebecca Hines: Yes. Someone whose name isn't really apparent.

Lorraine Doo: I will just find out their email. We will follow up with them separately. I think the guidance in the regulation is clear. We can follow up with them separately. That is right out of the CMS rule.

Stephen Konya: It is part of the reason why we have CMS involved at every level. We have them on the Executive Steering Committee, Coordinating Committee, on a few of the tiger teams. We are always looking for ways to bring in more CMS expertise to help guide us. We want to make sure we are not tripping over each other – that kind of thing.

Rebecca Hines: He said his name is Drew Hannah at Smile CDR.

You ready for one more?

Stephen Konya: Certainly. It looks like we got at least time for one more.

Rebecca Hines: I am not sure I understand the question. How much of a challenge is – to be able to get to government network when interoperability is established? Security-wise, how secure government network would be coming from outside?

Stephen Konya: I am not sure I quite understand the question.

Rebecca Hines: I don't quite get it. It is missing a few -

Stephen Konya: It almost seems like it might be implying a security question about government networks. I am not sure that is relevant to what we are talking about here. We are talking about just FHIR data transactions being able to be supported at scale. There is a Security Tiger Team, which is looking at trusted dynamic client registration, tiered OAuth, et cetera.

That is really looking at how to manage permissions and security across – you know, going between outside stakeholders. I mean, yes, there are a few government stakeholders that may be involved like

the VA and other healthcare providers, CMS. Largely, it is between – and maybe the Indian Health Service in some cases. Largely, it is going to be between payers, providers, public health professionals, others that are kind of not necessarily a government network.

I hope that addresses some of your question. I apologize if it didn't. Feel free to email me with more context.

Rebecca Hines: It was from a member of the public, so I do suggest you just email Stephen directly if you want clarity.

Any other questions?

I think we are good. Thank you.

Stephen Konya: Again, thank you to Alix for all of her involvement and the other members, Deb and Lorraine and others that are participating in all of these different efforts. We certainly value their contributions to the FAST, significant contributions.

Feel free to spread the word. Reach out to us if you think you can help out in any way. We really appreciate it. Thank you.

Chris Muir: Yes. Thanks everyone.

2020 NCVHS Workplan Review

Rebecca Hines: Bill, we are getting down – yes, so here is the workplan. Bill, did you want me to live edit this or do we want to just walk through it and make edits after? What would you like to do?

Bill Stead: Whichever is easiest because we sort of have a 15 minute block. Whichever is easiest for you.

Rebecca Hines: It is a question of really asking all of the members do you want to try to edit this now or do you want to just talk about it and edit it offline. Maybe we should just do that today.

Bill Stead: That is probably better.

Rebecca Hines: Okay.

Bill Stead: We talked through some of these yesterday. On the ones we have already talked through, maybe what we will do is just sort of say has anything changed there. That may be the way to do it. If you start with the convergence of administrative and clinical data, Alix and Rich, I think that is probably – still stays – is fine as it is.

Rich Landen: Rich, I think in the fourth quarter, we should probably add a bullet for data analysis. According to our three phases, we will get the ICAD output in September. After that, we start analysis.

Rebecca Hines: I am working on a live copy, Rich. I just added data analysis to Q4.

Rich Landen: Alix, you are okay with that?

Alix Goss: I am okay with that. The Q4 for the data analysis makes sense. We will probably have a preliminary set of recommendations in Q3. I think that with our focus on the rules from CAQH CORE, the timing I think is realistic to really take the deeper dive in Q4 for analysis.

Bill Stead: Okay. Then the other collaboration with ONC HITAC, that is good as it was. Shaking your head yes? Okay.

Predictability Roadmap I think TBD is a good place because we are – 14th report to Congress, the Executive Committee will work to have a – to be ready to have a discussion at the June Full Committee on themes and approach. So, that is still good.

The incoming change request, which was the Operating Rule that Alix just mentioned, we have got that hearing scheduled in Q3. So, that is good.

Evaluate the ICD-11 U.S. Modification Project. At this juncture, we are in monitor stage. We shared the updates yesterday.

PSC. Frank, do you want to suggest anything now to stub in to Q2 or Q3 or beyond based on – is there anything you want to stub in based on the conversation we had this morning?

Frank Pasquale: Yes. I think, basically, the last slide in my presentation had the two projects going forward, the first being the Trust Public Health Surveillance Infrastructure, the second one being on the unintended or unanticipated aspects or consequences of advancing interoperability. I think that both of those could go into both of those boxes, the 2020 Q2 and Q3 boxes as we meet together as a subcommittee to talk about the structure of the environmental scan and trying to find partners and also making sure that we are not duplicative of existing efforts.

Bill Stead: So you would be drafting the scope on Approach to Environmental Scan and Potential Partners probably for both of those with a first draft in Q2?

Frank Pasquale: Yes. That is right.

Bill Stead: And then, basically, based on that, in the June meeting, we would make decisions about path forward, which would then flow into Q3 and Q4. Is that – am I hearing your right?

Frank Pasquale: Yes. I think that is a very good timeline.

Bill Stead: Perfect. Okay. Data Access for Community. We did the logistical pieces. We have moved the Health U.S. Redesign – the next discussion of that to the June meeting.

Alix Goss: Bill, I am wondering if Margaret still has a question. I am seeing her hand raised and down. I wasn't sure if she was trying to chime in there.

Bill Stead: Good point. The hand is in a different place than I am used to seeing it, so I miss it.

Alix Goss: And Rebecca has been dutifully typing. Margaret, I am noticing your monitor change and your hand has gone up and down.

Rebecca Hines: Her internet went out and she has had some technical issues we have been dealing with on the back end. It might be from that. I don't know.

Margaret Skurka: (Inaudible)

Rebecca Hines: Margaret, if you have any comments, you can put them in the chat box, and we will read them out. Both Rich and Margaret are echoing badly. I think Rich was trying to get in before, but he was echoing a lot.

Rich Landen: I am not trying to get in. I have been on mute.

Rebecca Hines: Bill, I want to go back to the last row here now that we have that worked out. What were you about to say about data access for communities?

Bill Stead: All I said was that we moved, I thought, the Health U.S. Redesign to June, which is correctly reflected in the plan.

Rebecca Hines: Yes.

Bill Stead: We originally thought about that for March.

Rebecca Hines: Okay. Then it seems like with those minor tweaks then this is still pretty current.

Bill Stead: Yes, if we can find out what Margaret was trying to send.

Rebecca Hines: Right. Margaret, do you want to try again, or do you want to put any comment in the chat – questions in the chat?

Margaret says regarding ICD-11, nothing is listed in Q2, 3, or 4. As a newbie, asking are we waiting for HHS?

Bill Stead: The short answer is yes. We developed, as you know, the research questions and the recommended communication plan. At that juncture, as NCVHS, we didn't know how to do anything else until HHS came back with the results of that research or work with others to get that research in place. We would have to be informed by that before we could do the next part. Does that make sense to you?

Rebecca Hines: Her response is I just know that other countries are moving along. Canada, Japan for sure, and others, as I understand.

Bill Stead: Understood.

Rebecca Hines: Basically, Margaret, the committee did what it could. We just have to wait. There is really nothing more we can do. The Department clearly has some more urgent business that it is attending to this month. Thank you for having a chat/discussion with us.

The other point I just want to make – Maya, I don't know if you are on right now. We don't know what resources we are going to have starting in October. That is yet to happen. It is going to need to happen in the next few months. It hasn't happened yet. I cannot speak to how many full committee meetings,

how many subcommittee meetings, how much logistical support we will have. All of that is unknown at this point. I just wanted to make sure that all of the members are aware of that.

Maya Bernstein: Regarding budget, resources, that is what you were asking about?

Rebecca Hines: Just whether there are any updates on what we can look for later this year that will support the fiscal year starting in October.

Maya Bernstein: I don't know the answer to that. I will ask Sharon. I will say that – I mean, as everyone knows, the Department is upended by the virus. Whatever we have been doing – whatever schedule we were on, I think all of our resources – we have been asked to prioritize everything that is going to the virus first. Obviously, the budget needs to happen. We will get all of that together. In terms of how much – just generally, how much support the staff can give you, we are stretched. We may have to elongate some of the projects or rely more on the members to do some of the – I don't know – drafting, editing, whatever stuff that we used to do. Also, I know that you guys are stretched.

That is just a caution about the usual level of production that we can do. I don't know how it is going to go in the next few months. Obviously, the budget needs to move forward. Our leadership has already been doing budget hearings on the Hill for the upcoming year and so forth. I don't know that Sharon knows what is going to fall out of that yet for the fall – for the upcoming year's budget. But I will go and check.

Rebecca Hines: Great. Just for the new members, since I have been involved, things have shifted quite a bit. Over the years, the staff have played a really big role - Lorraine, Geanelle, Maya, Rachel, and previously Kate Brett, when Pop Health was more active. As Maya just said, the staff are really stretched right now. I am the only one where this is my main responsibility. I am not running a program. I am not providing policy guidance on another program. This is my primary responsibility. That is not the case for the other staff at all. So, just want to make sure you are all aware that they all have full-time jobs just like you do.

When we had more resources, we would hire consultants to write the environmental scans for us. That was super helpful. Then the subcommittee and staff would work with the consultant, guide the consultant. It is not clear what our ability is going to be to do things like that moving forward. It is just unknown at this point. I just wanted to make sure all of the members were aware of that situation.

Maya Bernstein: Right. We still may be able to do some of that – some of that hiring out. We have different pockets that we have to use in different ways. Yes, it is unknown at this point, but I don't want to be too pessimistic about it. We still may have the opportunity to hire some limited amount of consulting and writing and so forth.

Rebecca Hines: Beautiful. So all bets are not off yet. Very good.

Public Comment

Rebecca Hines: It is 2:45. It is time for public comment. I feel like Trevor Noah. It's time for – the instructions are coming up on the screen. They are also in your chat. If anyone has something they would like to convey to the Committee, now is the time to do it. If you are listening in through your computer on Zoom, you can click raise your hand to have your audio unmuted. If you are calling in

through the phone function, press star nine to request unmuting of your phone. As always, you can send comments to ncvhsmail@cdc.gov.

I haven't seen anything come in other than slide requests. We will wait a moment to see if anybody presses star nine on their phone or raises their hand.

(Pause)

Rebecca Hines: So at this time it does not appear that there are any comments from the public. As always, you can email us at ncvhsmail@cdc.gov. We will convey any input to the committee. Anything else we want to check in on before we adjourn?

Bill Stead: I just want to make sure that everyone realizes how grateful I am that people were able to engage so productively during this time. I think we were successful in moving forward the NCPDP requests in a way that the industry wanted us to. I think we have wrapped our head around both the next steps and the work around convergence. I think we got our head together around the plan for privacy, security, and confidentiality.

So, I think that we have done a good job. I know everybody had to do a lot of heavy lifting to get ready. I just want to make sure everybody knows how much I appreciate that. The heavy effort of the staff, both the National Center and ASPE help that we have had, and the help from RLM Associates - this has all worked extraordinarily smoothly. I guess I would be remiss if I also didn't say Rebecca has been an unbelievable champion as we have worked our way through this. Thanks, everybody. From my perch, we are done.

Rebecca Hines: Not quite. Well, we can adjourn, but before we do I just want to echo what you said, Bill, and personally thank Marietta Squire, Geneva Cashaw, Maya Bernstein, Rachel Seeger, Lorraine Doo, Geanelle Herring, and all of the other people who in other ways have supported all of this. And then, of course, Rose Li and Associates, in particular, Greg Richards and Kim Williamson. This really is team sport, as I like to say. I think the team just – a touchdown today. Thank you all.

After we adjourn, I would like to hold on and do a little quick discussion about the logistics. Let's formally adjourn, Bill.

Bill Stead: We adjourn the public meeting.

(Whereupon, the meeting adjourned at 2:50 p.m.)