Health Information Technology Advisory Committee
Office of the National Coordinator for Health Information Technology

Annual Report
Work Group

Transcript
November 9, 2018
Virtual Meeting

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Good afternoon, or good morning for some of you, and welcome to the HITAC's Annual Report Workgroup meeting. I believe this is now our fifth meeting so we will call the meeting to order starting with roll call. Carolyn Peterson?

Carolyn Peterson – Individual – Co-Chair

I'm here. Good morning.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Hello. Aaron Miri?

Aaron Miri – Imprivata – Co-Chair

Hello and good afternoon.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Christina Caraballo?

Christina Caraballo – Get Real Health – Annual Report WG Member

Hi, I'm here.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Hello. Brett Oliver?

Brett Oliver – Baptist Health – Annual Report WG Member

Here. Thanks.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Great. And Chesley Richards?

Chesley Richards – Centers for Disease Control and Prevention – Annual Report WG Member

Here.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Perfect. Okay. So, we have a full group today and I will turn it over to our co-chairs, Carolyn and Aaron.

Aaron Miri – Imprivata – Co-Chair

Sorry. You want to start?

Carolyn Peterson – Individual – Co-Chair

Go for it, Aaron.

Aaron Miri – Imprivata – Co-Chair

Okay. I'll start. I want to thank everybody for joining us today. We have a pretty full agenda to talk through. This is a topic, personally, that's very near and dear to my heart with privacy and security, particularly. And really understanding where we're going to go with this, in terms of opportunities, in terms of gaps, in terms of where the market, where the sector, where the vertical is going. As a hospital, the healthcare CIO, this is on my plate every single day, top to bottom, so I'm very appreciative of our speakers today and appreciative of this task force being able to look at this and really being able to assess and understand and really dig deep into this very important topic. Carolyn?

Carolyn Peterson – Individual – Co-Chair

I absolutely agree. I think all of the committee members here and also within HITAC have expressed great concern about privacy and security and see it as a primary issue and consideration for HITAC and for ONC, particularly as it supports the focus on consumers being able to access and use their data and greater interoperability. So, I'm really pleased that we can have these presentations today and have a more rounded and deep discussion about this issue so we frame it well in the annual report.

Aaron Miri – Imprivata – Co-Chair

Okay. Carolyn, do me a big favor and get started with this. I'm trying to reboot my computer as we talk.

Carolyn Peterson – Individual – Co-Chair

Gosh. I'm sorry. I know how that works. Let me start by reviewing the agenda. We're going to take a deeper dive into privacy and security priority target area this morning. We will have three presentations.

First, Linda Kloss, the chair of the subcommittee on Privacy, Confidentiality, and Security with the National Committee on Vital and Health Statistics, will share with us “Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges.”

Then, Kevin Stine, chief of the Applied Cybersecurity Division, Information Technology Laboratory of the National Institute of Standards and Technology, will share with us the NIST Cybersecurity Framework.

Finally, we’ll have Nicholas P. Heesters, Jr., Health Information Privacy Security Specialist of the HHS Office for Civil Rights, share with us the OCR cybersecurity resources. These are some things that were sent out and included as the background material for our discussion today but they’ll be helping us work our way through and understand what the high points are of those materials.

Then we’ll move to a workgroup discussion among the members. We will discuss planning for a workgroup update at the HITAC meeting to be held soon. And then we’ll have a public comment period and go with next steps and an adjournment. So, with that, I’d like to hand the floor to Linda Kloss to begin her presentation on “Health Information Privacy Beyond HIPAA.”

Linda Kloss – National Committee on Vital and Health Statistics – Privacy, Confidentiality, and Security Subcommittee Chair

Thank you and good afternoon. I’m very happy to be representing NCVHS and helping the annual report group frame their important annual report. Next slide, please. We’re gonna move through this agenda pretty quickly so there’s time for all three speakers and time for discussion.

My goal would be, first of all, to highlight some of the findings from our recent environmental scan, “Health Information Privacy Beyond HIPAA.” I’ll give a little context for that work first and then some of the highlights, discuss what the National Committee is now doing to kind of continue and act on, move on what we learned through the environmental scan, and then suggest how this work might inform your annual report or at least some areas that seem like some reinforcement and further work could be very helpful. Next slide, please.

Just by way of background and as a reminder, NCVHS is a federal advisory committee. It was established in 1949 and its focus is on health information and data policy. So, our scope is health data, statistics, national statistics, vital statistics, privacy policy, and the Department’s strategy to address those issues. In 1996, the Committee received an additional charge to assist and advise the Department in the implementation of administrative simplification provisions of HIPAA. Of course, that’s transaction standards and the privacy and security rules. And, thirdly, to inform decision making about data policy.

So, generally, the report out from NCVHS is a series of letters to the Secretary or reports, such as the environmental scan we're talking about. So, we have kind of a broad charge and often the Committee will decide what the collective experience of a multidisciplinary committee is seeing as real issues in the field and take up those issues. And this work, beyond the HIPAA initiative, really grew out of previous work. For example, in the recent years, the subcommittee has worked on access and disclosure of health information with a focus on release of information. What's this notion of a minimum necessary release? We've done a deeper dive into de-identification. NIST helped us and informed our thinking in that work. And we've issued letters to the Secretary on that. And I'll come back to a couple of those because I think there are some areas that can bridge the work that you're doing. And we've done a lot of work recently on uses for health data to improve health in the community. And as we did that, we're kind of out of the space of HIPAA, if you will. Next slide, please.

So, we began to think we really should take a broader look at privacy challenges outside the regulatory scope. And we struggled some with what to call this initiative. Initially, we labeled it HIPAA 2.0 but that kind of connotes that we're looking at scrapping HIPAA and building something new. And I think we started out here with an assumption that HIPAA is adequate for what it's doing, in terms of protecting health data in the hands of covered entities that are subject to HIPAA., but that the challenge that we face as our information becomes liquid and more ubiquitous is all of the area that is beyond the scope of HIPAA.

So, we set out to identify and describe this changing environment and that's the environmental scan that I've referenced in the title to this. And I'll give you the link in just a moment. And then, based on what we learned, to consider what the integrated models are for how we might protect privacy and secure health data outside of the HIPAA protections while certainly enabling use and service and research and all of the other improvements that we're looking to health data to provide to us, and formulate recommendations for the Secretary, as NCVHS does. But also probably because of what we might learn in the course of this, we set out a goal of then preparing a report for health data supports and meaning that broadly.

So, this was to be broadly directional work and it emerged from the Committee's work over the past several years. For example, the work that we did in looking at the adequacy of HIPAA de-identification protections really revealed that we shouldn't be as reliant or assume the reliance on de-identification. That re-identification is with us. It is a reality. It's only going to get easier as more and more data sets converge and as new tools develop. This world then, beyond HIPAA, is broad and growing. And as you well know, the U.S. has a sector-specific health information privacy and security law in a world where data is liquid. So, really, we set out in the scan to understand the current environment better. Next slide, please.

We tackled these topics and the link there to the report is shown. We looked at big data and the expanding uses and users; personal and medical devices and the Internet of Things. We overviewed laws in other domains. Where might there be laws that could help us deal with the issues in this world beyond HIPAA? Evolving technologies for privacy and security and evolving consumer attitudes. What you don't see on this list is cybersecurity. We deliberately set that aside because of the work of NIST and because of the recently published Cybersecurity Taskforce report and, really, in some part, because of bandwidth, but not because it wasn't critically important.

We approached this scan by holding two hearings. We learned from experts, both in the private sector and government and quasigovernmental agencies. And when you review the report, I think you'll see that one of its really important uses is that it brings together a number of really important industry reports on topics that are relevant in this space. So, I think that's one of the important contributions. I want to make a special call out to Bob Gellman, who served as primary author of this report. Bob is an attorney and a former member of NCVHS. He's a real expert on health information privacy and I'm not sure we could have succeeded at bringing together the full array of issues in this space without Bob's help. Next slide, please.

So, key themes. And these are kind of important to keep in mind and I think they have some relevance for the work that you're doing. We made the distinction between the regulated world subject to HIPAA and the unregulated world. It's not a very fancy way of making this distinction but we wanted to underscore that, for the most part, the unregulated world is not subject to any specific regulatory or statutory regulation for privacy in the U.S. at this time. And we noted that the data in the unregulated category are, for the most part, not subject to statutory regulations but that those boundaries between the regulated and unregulated are most certainly blurring.

We described the growing challenges of defining health information: its ownership, control, and consent issues. There's a broad range of organizations, as we know, that rely on health data as an element of a commercial activity or other kinds of activity: data brokers, advertisers, websites, marketers, genetic testing firms, and others. It's hard to estimate the size of the unregulated world but we know that just the area of analytics is estimated to be $9.5 billion by 2023. So, the unregulated world is vast. And what we tried to do, and I think Bob did particularly well, is incorporate selected stories of this unregulated world, illustrating potential risks and harms in these areas of big data, personal health devices, Internet of Things.

What we didn't do is lay out specific recommendations. That wasn't our charge. This is really an environment scan. But we did look at what kind of frameworks or mechanisms might be available to increase protections and choice, either regulatory or principles or stewardship protocols, and at the same time, reduce burden. And we took a little bit of a look at what the legislative issues and approaches, such as general data protection, might be in this space. So, this is a 68-page report but it is readable and I encourage you to, most certainly, at least scan it. And we thing that its contribution is to bring together, in readable form, a lot of really complicated concepts that are challenging to us all.

Where the Committee is now, and I'll just take a couple of minutes to do that and then turn it over to my colleagues, is to say, "What does all this say to us?" Next slide, please. So, we are kind of designing right now or framing, if you were, some models that bring together the lessons from this environmental scan. We're not describing this as a legislative approach. We're at this point kind of calling it a stewardship continuum. And what we understand is that all the players, from those that are in the regulated space – the HIPAA-covered entities or business associates – to all those who are data holders, that there are steps that can be taken to do better with privacy. And we think that the mechanisms are both public actions – legislative, regulatory – but also private actions. And so we have kind of begun to frame out what – when we're in the HIPAA-covered entity space, we're kind of focused on compliance risk. But when we're in the unregulated space, we're really looking at use, disclosure, risk, or risk of harm. And what we felt when we finished the report was that there are some areas that kind of are at the intersection between the regulated and unregulated world that we might learn something from. Next slide, please.

And so we've taken kind of three use case areas and begun to take a look at them: data registries, personal health devices, and geo-fencing apps or apps that can infringe on privacy. And use these as examples because they can kind of live at the intersection, if you will. For example, we know that some health data registries are treated and have business associate agreements. Others do not. Why the difference in practice? What are the implications of that difference of practice? Personal health devices, you'll be certainly hearing more about that in just a moment. Can't there be some minimal standards for privacy and security of this information, particularly as it moves from the device into the regulated environment and so forth? So, we're kind of starting with this area at the intersection and we think that this is probably a pretty practical way to commence and I think that has some lessons for the Annual Report and the focus for ONC. Next slide, please.

And then we're kind of drilling down into what kind of mechanisms exist, both public and private, in those intersection spaces. And I won't take time to go through this but you can see that there are things that can be done. There are mechanisms, such as requiring that registries become covered entities if we're going to release data, even deidentified, knowing the risks of re-identification, to a registry. And, most certainly, HHS has some levers that can help with that. Next slide, please.

So, where we've come on our beyond HIPAA journey is to publish the environmental scan, explore these exemplars that work at the intersection, and begin work on framing some models. And we, as a committee, have our own obligation to produce an annual report to Congress on the state of HIPAA so we'll be including some themes here. But we're planning for a hearing to look at modeling and to think about how we can, through both public and private partnering, work together put in some sensible guidelines for the world beyond HIPAA. And we'll hold a hearing in the spring and then produce a letter to the Secretary. And it's kind of a learning journey but we hope we're making some progress and we hope that this informs your thinking.

And I think there are several areas to take away. Reinforcing this privacy landscape – we just can't think about HIPAA as being the solution to healthcare information privacy anymore. It's part of it. It's adequate where it applies but it's not comprehensive, most certainly. What is the technology that can be spotlighted to help with the privacy and security challenges? Anchoring some of your work, most certainly, at this intersection, be it interoperability, exchange, or devices. Reinforcing the recommendations that NCVHS has made about de-identification and where our policy work in that regard needs to go next. So, I think I'll stop there and certainly look forward to any questions as the speakers conclude. Or do you want to take them now?

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

I think we have time for a couple of quick questions, Carolyn or Aaron, unless you disagree. Otherwise, we could proceed to the next speaker.

Aaron Miri – Imprivata – Co-Chair

I would say we probably ask a few questions in between and then we can wrap it up with more questions about everybody after everybody finishes. That will give everybody a chance to go through it.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Great.

Aaron Miri – Imprivata – Co-Chair

Okay. I'll start. First of all, thank you very much. This is an excellent presentation and I appreciate the work that NCVHS has been doing and I really appreciate your thought of framing it. I found myself taking some notes here about how I'm going to frame some discussions at my health system based upon how you were presenting the various scenarios. So, thank you for that.

My question for you is to what degree did you guys consider data exchange internationally? Obviously, you mentioned GDPR and some of the components there but even I'm finding, as a healthcare CIO, the amount of patients coming into this country to receive the top-tier care and then going back home to their home country is becoming a bigger issue, especially as you now deal with various applications reaching, via API or whatnot, into data sets. And so did you guys look at that in any detail and how that data liquidity is starting to affect privacy and security?

Linda Kloss – National Committee on Vital and Health Statistics – Privacy, Confidentiality, and Security Subcommittee Chair

Well, we addressed GDPR briefly in the report. We also addressed in more detail the principles of fair information practice, which, of course, underpin HIPAA and GDPR, and kind of anchored once again the importance of those principles in everything we do and how we build these frameworks. Since we finished the environmental scan, of course, GDPR has gone into full effect and the Committee has had a subsequent briefing about GDPR and about the California consumer protection statute that is modeled on GDPR. And we have heard from experts that have testified to the Committee on this topic that, really, the rest of the world is looking very closely at a data protection approach. And when you look at that framework I just threw up briefly, a data protection model is certainly one of the alternatives that we'll be exploring.

So, I think this is evolving but I think you're absolutely right and I think that somehow we need to, not necessarily replace HIPAA, which works well for what it works well for, but append to it. And I think as we've looked at this, we've kind of taken some lessons from NIST and their thinking that we need to focus in this unregulated world on risk and harm and also how to reinforce consumer choice in a more expanded way than we have. So, I think there are absolutely elements of that that will continue to be discussed by the committee as we go forward. But you're right. This approach is here and I think most healthcare systems are beginning to say, "How does this affect us?"

Aaron Miri – Imprivata – Co-Chair

Exactly. Thank you.

Carolyn Peterson – Individual – Co-Chair

This is Carolyn. I have a follow-up question on your previous comment. You had mentioned a need to focus on risk and harm. I'm wondering if you can tell us more about that perspective. I know one thing that I have heard and that I see sometimes in writing, particularly those that have some legal bent to them, is, "What's the harm? Prove to us that there was a problem from whatever the action was that someone purports violated their privacy rights or violated confidentiality." How do we assess harm in this environment?

Linda Kloss – National Committee on Vital and Health Statistics – Privacy, Confidentiality, and Security Subcommittee Chair

Well, I'm not sure I can answer that today. One of the recommendations that we made in the de-identification letter to the Secretary was that, in fact, we need to be doing some additional research and modeling into how to do just that. We understand what the risks are but how do we apply that in a situation of assessing harm. I think it's an area that needs more work and we identified that in the context of use of deidentified data and I think it's applied here in a much broader context.

Aaron Miri – Imprivata – Co-Chair

This is Aaron. I just want to ask a really quick follow-up on that. Instead of, or maybe amending, the word "harm," can we call it accountability? Because as a committee, we have talked about the concept of accountability and what that actually means. So, I can see harm in terms of if we're talking about quality, patient care, and outcomes, but there's also the accountability, as to where does the ball land, per se, if there is an issue around EPHR or whatnot. Is that a fair statement?

Linda Kloss – National Committee on Vital and Health Statistics – Privacy, Confidentiality, and Security Subcommittee Chair

Well, going back to the fair information practices, I would say they're different and both important, of course. But I think harm is what happens if databases are merged and we target a particular area where there's some cluster of health problems. We've seen this, certainly, historically and property values go down. There are ways to judge real harm and I always go back to the risk and harm model that NIST has put forward. Loss of autonomy comes at some peril to the individual and I think there needs to be some way of describing harms from inappropriate information use. And accountability, of course, but I think they are different.

Aaron Miri – Imprivata – Co-Chair

Got it. Thank you.

Carolyn Peterson – Individual – Co-Chair

Do we have questions from other members of the workgroup?

Christina Caraballo – Get Real Health – Annual Report WG Member

This is Christina. I don't have a question but more of a comment. I was specifically interested in the approach to look at the unregulated work and also looking at, specifically, the personal health devices. I think this is going to be increasingly important for consumer engagement initiatives and as we move to our goal of consumers being able to have the ability to use the app of choice when interacting with their health information. So, I definitely am curious to learn more about that and see how we can incorporate some of the work that you are doing to help guide us in our consumer access pieces.

Linda Kloss – National Committee on Vital and Health Statistics – Privacy, Confidentiality, and Security Subcommittee Chair

I agree. One of the realities that we pointed out in the report is that information, no matter where it is, it's just difficult even to begin to identify who has the information and then, of course, over time, how accurate it is and how it's being used. But, most certainly, for devices, the accuracy of that information and the security of that information is paramount from any useful purpose to the healthcare field. That's why I thought that anchor of the medical device and technology really is probably a real sweet spot for ONC.

Aaron Miri – Imprivata – Co-Chair

Good deal. Thank you. Anybody else on the committee real quick? Okay. With that then, I want to thank you very much again. We really appreciate that. This was an excellent presentation. Should we move on then to the next speaker?

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Yeah. Let's go ahead and do that.

Aaron Miri – Imprivata – Co-Chair

Okay, Kevin. You're up.

Kevin Stine – National Institute of Standards and Technology – Applied Cybersecurity Division Chief

Thank you and thanks for the opportunity to speak with you today. I'm happy to share a little bit and kind of scratch the surface on this broader cybersecurity program, maybe provide a little bit more context on the Cybersecurity Framework. I think a lot of the discussion so far around risk management as one of those core principles, if you will, is certainly something that we hold very, very dear, if you will, within the NIST portfolio of the cybersecurity and privacy. So, I look forward to a good discussion.

So, if you can go to the next slide, our purpose at NIST, if you will, with respect to cybersecurity and privacy is really to help, in some ways, cultivate trust in information and in technology. And we do that through advances in cybersecurity and privacy standards and technology and measurement science. Our focus and our portfolio, if you will, kind of spans from the early-stage foundational research of next-generation cryptographic technologies, for example, all the way through to the application of that research and those technologies in ways that help organizations to really understand, manage, and communicate risks in the context of their missions and business objectives.

We do that in a very open and transparent way, kind of focusing on the development and promoting the use of standards and best practices and other tools. And, again, done in a very open and transparent and in a non-regulatory and non-prescriptive way, really focusing in on that principle of risk management because each and every organization is unique in some way. While we have a lot of commonalities, there are certainly things that are unique among us. I'm going to go to the next slide.

Again, from a broader NIST cybersecurity and privacy perspective, we have several big buckets, as I like to think of them, and here are just a few of those right there. But I'll really hone in on that top one, which is we seek to equip organizations, whether they be federal government agencies or other layers of government, even international; industry; different verticals; small businesses; and in this context, maybe small providers. We help organizations better manage cybersecurity and privacy risk, really identifying those integration points between cybersecurity and technologies and information and the business or the mission, purpose, and value. Go to the next slide. Thank you.

That's really where the Cybersecurity Framework, kind of the sweet spot where the Cybersecurity Framework plays. Maybe just a little bit of background on our original charge or charter in that space. It did stem from an executive order in February of 2013 to work with critical infrastructure sectors – at the time, 16 defined sectors – to produce a performance-based, voluntary tool to help organizations understand, manage, and communicate cybersecurity risks. Again, in the context of their missions and business objectives, and to leverage standards and best practices to help them do that.

What we've seen since then, not only has the charter of the framework been kind of enhanced, if you will, beyond just an initial executive order, it's really now codified our role in this space with respect to ownership and evolution of the framework through the Cybersecurity Enhancement Act of 2014. It really helped to drive home the value of that framework and the attributes that the framework provides. But we've certainly seen the community well beyond the defined critical infrastructure sectors and well beyond just the bounds within the United States, the geographical bounds of the U.S., uptake not only the framework but I would say, more importantly, the principles that the framework embodies with respect to a risk-based approach that really aligns the cybersecurity needs of the organization tightly with the mission and business objectives. We think that's a valuable characteristic. We'll go to the next slide.

So, let's kind of unpack what the framework is real quick and I'm sure many of your organizations have either heard of or are familiar with it and maybe you're even using it. That would be great. So, simply put, we view the Cybersecurity Framework as a tool to help organizations understand, manage, and communicate cybersecurity risk. There's a lot of core attributes, if you will, of the framework that we think are very important and I think these attributes have certainly helped to increase the utility of the framework and the broad adoption of the framework in a lot of different ways by different types of organizations.

I think perhaps the most significant value proposition of the framework is that it provides this common and accessible language. Us cybersecurity people, we're very good at talking to other cybersecurity people about cybersecurity but when we introduce more of the alignment of cybersecurity to the actual mission and business objectives of an organization and the priorities thereof, we're talking to folks unlike us, for example. So, we need to be able to have a tool or a way to have that common language, that common dialogue that can span multiple types of individuals and functions within organizations and sectors and even nationally and internationally as well.

It's definitely something that's meant to be adapted to different types of technologies, to lifecycle phases, to sectors, to different types of organizations. And, increasingly, we're seeing that from governments as well. It's certainly meant to be customized. The framework is a great starting point but really tailoring it or customizing it in a way that's going to be the most relevant and applicable to your organization and your organization's needs is tremendously valuable. And that's really where a lot of the value is kind of derived.

It's also meant to be paired. The framework, at a high level, provides a collection, if you will, a catalogue of cybersecurity outcomes that are presented in a kind of plain language way. A kind of non-technical, non-geek kind of way. It does not actually provide a how or the how much, in terms of how much cybersecurity is appropriate for an organization, but, again, provides that collection of outcomes that, based on your organization's priorities, your assessment of risk, your threat landscape, all those types of things help to inform an organization, not only on their use of the framework but really in their cybersecurity risk management approach and aligning it, again, with the missions and business objectives.

Certainly, it's a living document. I think everyone knows that this space changes rapidly. Certainly, it's something that needs to evolve with changes in technology and the ever-changing threat landscape and it has to evolve along with those.

And I think part of the last piece on this slide is just that this common language is anchored in five very simple terms and they're depicted in the graphic on the right of the slide – the five functions, we call them – identify, protect, detect, respond, and recover. And those five words are meaningful to many different audiences, whether you're the data center folks developing systems or you're the executive that may not have a cybersecurity background but certainly is involved in many types of risk management decisions, whether those be financial or reputational or safety or other types of mission risks. Cybersecurity is another risk dimension that needs to be included within that discussion. And those five words resonate with many different types of communities. So, again, that common language approach. Go to the next slide.

So, drilling down into a little bit more detail, the Cybersecurity Framework has three main components. The first is what we call the Cybersecurity Framework Core. And, again, that's really that catalogue of cybersecurity outcomes and associated informative references. When I say informative references, those are the collection of standards and best practices that would help an organization achieve a particular cybersecurity outcome that they prioritized, again, for their organization, as aligned with their mission and their business objectives. Also, it's primarily that common language that helps to enable that communication of cybersecurity risk and cybersecurity activities across an organization. Go to the next slide.

The second component is the Cybersecurity Framework Profile and this is really where that alignment happens, where you take that Cybersecurity Framework Core that we just talked about – again, that general catalogue of cybersecurity outcomes and informative references, the standards and best practices – and where you're aligning those industry standards and best practices through the core to a specific implementation scenario. And that could be for a sector as a whole, and we have a lot of examples of sectors coming together to do that, as well as many specific organizations. And I'll have some examples later on in the slide deck that will kind of point you to some examples of how organizations have taken this.

But this is the tool where you're really customizing the framework to meet your specific needs as an industry, as a specific organization, as a solution provider. For example, when you want to be able to articulate in a common way or an easier to understand way how your products and services would help an organization achieve a particular cybersecurity outcome. But, again, customizing the use of the framework in a way that's meaningful to an organization that takes into account their business objectives, their threat environment, and their requirements or controls or different regulatory regimes, for example. And the output of that alignment is a Cybersecurity Framework Profile. Next slide, please.

The final piece or component of the framework is what we call the framework tiers or the implementation tiers. And this is really just a progressive set of characteristics that would describe how cybersecurity risk is managed by an organization and the degree to which those risk management practices are integrated into broader enterprise risk management activities. Again, risk management processes and other agreed to integration into the broader enterprise activities, as well as what we call external participation. Are you just ingesting information from other organizations, for example? Are you able to take information in, apply it in meaningful ways to your operating environment? Are you able to provide information back out based on what you're seeing and providing that to the broader community to help improve the overall state of the ecosystem, for example? While not necessarily a maturity model, there's certainly a progressive evolution from a Tier 1 – what we call a "partial" – up through a Tier 4 – adaptive. Much more agile. And the key takeaway for the tiers, however, is that it's not always a race to the top. There is a cost dimension that comes with being at a certain tier for a certain capability and that's certainly something that each organization should keep in mind. Let's go to the next slide.

I think this notion of true enterprise risk management is one, again, that I mentioned before, and we hold that very near and dear. It's extremely important because cybersecurity, in and of itself, is, in the broad picture, another type of risk that all organizations are trying to manage. I think the key value proposition of the Cybersecurity Framework is to support risk management, both vertically within an organization, from, again, that senior executive level through the business process level down into the implantation and operations level – and this is bidirectional exchange of information that's informing activities and decisions at all levels – but not just vertically within your organization but also horizontally with your partners and suppliers. When you think about the supply chain dimension that is certainly a very critical topic and certainly a very hot topic today, the value of the framework to be able to express expectations and capabilities horizontally within the supply chain, regardless of your organization's role within that supply chain, is tremendously valuable.

I guess in February 2014, we issued Version 1.0 of the framework and we've seen significant uptake over the last several years, as well as a significant evolution, as I mentioned, in the technology landscape and the threat environment and, really, increased interest in and awareness of cybersecurity at all levels of the organization. That interest and those uses of the framework over the last several years certainly helped to inform and drive an update that we recently issued back in April of 2018, what we call Version 1.1. And that update reflected a few major changes or a few major evolutions, if you will, of the framework. Certainly, an increased treatment of the supply chain topic. Again, that's one that's of critical importance and it is kind of popping up in any and all sectors and broadly between nations and internationally as well. Certainly, an increased emphasis on measurement. But measurement in the context of self-assessment. An organization being able to take a look at where they are today, where they need to be based on their assessment of risk, and helping to chart a path, a prioritized path to close that implementation gap, if you will. And let's go to the next slide.

So, here are a few sample resources that I wanted to highlight, more just to illustrate the depth and breadth of the uses of the framework today. This really is just scratching the surface. We've seen many nations adopt the framework. I think, at this point, we've had engagement with probably 50-60 individual nations. Many of those engagements have been for raising awareness. Certainly, we've got probably close to 30 nations that have, in some way, shape, or form, adopted the framework to support their national cybersecurity activities. National cybersecurity strategies, for example. One that I'll highlight is the Italian government has essentially adopted the Cybersecurity Framework, whole cloth, to support their national framework for cybersecurity. Other nations, such as Israel, Bermuda, Japan, a variety of other nations – Uruguay, for example – have essentially done the same thing because they see the value in a risk-based approach, a risk-manage approach, and view it as a valuable tool. Other sectors as well: water and waste treatment, financial services, telecommunications. All of those sectors have adopted the framework in a variety of different ways and have produced, in some cases, derivative guidance or case studies and custom profiles that have been providing value. Next slide, please.

The healthcare sector – healthcare and public health sector – is certainly one of the sectors that's been kind of an early adopter, if you will, of the framework. And there are many derivative works or example uses of the framework that have been produced and are shared out there. I mean, the framework is certainly a community effort. It was a community effort to develop the framework and continue to maintain it and these types of work products and example uses provide a tremendous amount of value. Here are a few that you can see here. Again, at the end of the slide deck, there are a few web resources that will take you to a much more complete and ever-expanding set of industry resources or actually just resources that come from industry, from specific sectors and organizations, and from government agencies as well.

I think with respect to the healthcare community, I think the top resource there on this list that certainly garners a lot of attention is the mapping between the HIPAA security rule and the NIST Cybersecurity Framework. And part of, again, the value proposition of the Cybersecurity Framework, is because it has that higher level common language or taxonomy for describing the universe, if you will, of cybersecurity activities, it's a nice mapping point or point of integration or alignment and harmonization between a variety of different rule sets, whether those be organizational policies or international standards or different compliance and regulatory regimes. Having that common language allows that accessibility to a variety of different ways to demonstrate alignment. We'll go to the next slide.

I wanted to just take a quick minute and talk about another point of collaboration that we have that continues to grow with our engagement with the healthcare sector. And I think the framework, in many ways, is the on-ramp to our National Cybersecurity Center of Excellence. And the way I like to think about the NCCOE – or the Center, in simple terms – is that organizations face challenges today with respect to cybersecurity. And there are many types of technologies or solutions out there that could help organizations address those challenges. There are cybersecurity challenges that are impacting their missions and their business objectives. At the Center, we seek to accelerate the adoption of secure technologies in ways that are aligned with the business challenges of organizations. Go to the next slide.

Part of that approach is to really work with, in this case, the healthcare sector, for example, to understand – and what we call our "community of interest" – to understand what are some of the specific healthcare challenges or cybersecurity challenges that are impacting healthcare communities as a whole. After we're able to kind of scope the problem, if you will, we continue to work with the healthcare community and with vendors of different types of products and technologies, which if integrated in the right way, can help address or provide an example solution to help address that particular challenge.

One of the more mature sectors that we work with at the Center is, in fact, the healthcare sector and here's an example of three projects, actually in order of when we worked on those. The first being securing electronic health records on mobile devices, where we actually, in all these cases, have provided very detailed example solutions on how organizations can use available technologies to help address a particular need. Most recently, we issued an example solution around securing wireless infusion pumps. And in doing that project, we worked with five infusion pump manufacturers that represented roughly 85% of the infusion pump market within the U.S. so that's a pretty significant touchpoint, if you will. Recently, we just embarked on securing picture archiving and communications systems project, and we, just within the last couple of weeks, announced the different companies and PACS manufacturers that we're working with through that effort as well. Certainly, sharing these for your awareness but also, certainly, your participation in these and potentially future projects that we'll embark on at the Center in the healthcare portfolio. We can go to the final slide.

I’m not sure why I kept this one in but, anyway, today is actually the last day of the Cybersecurity Risk Management Conference. But I wanted to put it up there because, one, I guess a lot of the information that was generated, either leading up to this conference but certainly coming out of it, will be posted both on this event site as well as on the Cybersecurity Framework site and other resources as well. And there is significant healthcare participation in this particular event. Not just healthcare specifically, many other sectors as well, but I think a lot of the lessons, because of the commonalities that many types of organizations share, a lot of the resources and the outputs of the discussions here at the conference over the last few days could be certainly applicable to any and all organizations across a variety of different sectors as well. And if we could go to the final slide?

I’m certainly happy to take any questions. I think many of the resources, certainly all the resources I just mentioned, are available on the variety of websites here, including work on our emerging Privacy Framework that we are embarking on and just started recently. And, again, my contact information is there and I certainly welcome any questions that you may have.

Aaron Miri – Imprivata – Co-Chair

Kevin, thank you very much. This was an excellent presentation. I greatly appreciate it. I know we’re going to kind of be abbreviated here because we want to give time for the next presentation and so forth. I just want to ask a very quick question to you. You mentioned quickly about the countries that are adopting or have adopted wholeheartedly the NIST Cybersecurity Framework, such as Italy and others that you mentioned. One of the topics we have talked about as a committee looking at this, as a taskforce looking at this, is the potential for further embracing the NIST Cybersecurity Framework at sort of that minimum threshold that this is the right path and that we should nationally adopt the Framework and say that this is that speed limit to the highway. Today, as you know, NIST is suggested and recommended but it’s not mandated, it’s not required, so there’s no minimum floor, per se. Would you say that the countries that have gone all in and said that this is the minimum floor – do this or better – have fared better against attacks such as WannaCry and others? And would you say that that’s probably the preferred route in terms of implementing a framework?

Kevin Stine – National Institute of Standards and Technology – Applied Cybersecurity Division Chief

So, I would say it would be hard to determine. Many of the countries are in different stages of their acceptance and implementation. It would be hard to say with any certainty that use of a particular framework, whether it’s NIST or ISO or another one – the correlation between use of a framework and attacks, for example, and what the relationship is there. I think what many of the nations are observing and gleaning benefit from the framework is less about making sure you do these things and serving as the floor and more about really embracing the principle of risk management. Many of the discussions that we have with other nations – quite honestly, a value for us is if we can make it through an entire discussion without actually talking about the Cybersecurity Framework but more about the properties that the framework embodies – a risk-based approach, a prioritization approach, something that’s cost effective and aligned with the needs of the organization. There’s certainly a lot of value there. And I think many of the nations, while many of them have very different approaches to cybersecurity, in terms of heavily regulated versus, in my work, more of the free market, if you will, and different approaches there, and I think we're seeing a lot of different approaches from different nations that align with their cultural aspects and preferences and the ways in which government and industry work together. But certainly many of them are very early on in their implementations and I think the Framework is a great starting point for providing that common dialogue around cybersecurity.

Aaron Miri – Imprivata – Co-Chair

Excellent. Thank you. Anybody else real quick on the committee?

Carolyn Peterson – Individual – Co-Chair

Yes, this is Carolyn. I have one question. Kevin, thinking back in your presentation about the five words in the Framework, it strikes me that that might be useful for this annual report because they're meaningful and applicable to multiple audiences, which is, of course, our goal, as it is yours. I'm wondering if any caution about that approach or any considerations we should take into account come to mind.

Kevin Stine – National Institute of Standards and Technology – Applied Cybersecurity Division Chief

We at NIST try to use those five words in a lot of different ways as well. And in some ways, we try to organize our portfolio around them also. And I'm familiar with other organizations that have taken a similar approach. I wouldn't have any particular caution that comes to mind with respect to organizing your annual report or other types of resources around those five words because we have observed that they are meaningful to many different types of organizations and roles within organizations. So, if there's a way to kind of anchor it to those five commonly accepted terms and commonly understood terms, I think that you're well on your way breaking down some of the communications divides.

Carolyn Peterson – Individual – Co-Chair

Great. Thank you.

Kevin Stine – National Institute of Standards and Technology – Applied Cybersecurity Division Chief

Sure. Thank you.

Carolyn Peterson – Individual – Co-Chair

Let's move on to our third presentation with Nicholas Heesters.

Nicholas P. Heesters, Jr. – United States Department of Health and Human Services Office for Civil Rights – Health Information Privacy Security Specialist

Hello, everyone, and thank you for giving me the opportunity to talk about the cybersecurity resources that the Office of Civil Rights produces and has out there and available to help protect health information. So, I am Nick Heesters and I work in the OCR Health Information Privacy Division, as part of our team that works on HIPAA compliance and enforcement for our regulated community. Next slide, please.

So, just a few of the resources that we have out there that I was going to touch upon for this presentation: the aforementioned HIPAA Security Rule and the Cybersecurity Framework Crosswalk, some of the other cybersecurity guidance materials that OCR has available on its website, as well as the recently updated ONC/OCR Security Risk Assessment Tool. Next slide, please.

So, as Kevin already mentioned, there is a Crosswalk available from the HIPAA security rule to the NIST Cybersecurity Framework. This is not guidance material but it's a voluntary tool to help organizations manage risk while also being able to assure that they can assure the protection of health information and service delivery. This has been a collaborative effort between resources at OCR, ONC, and NIST. Next slide, please.

So, this Crosswalk was released in February of 2016 and the way that the Crosswalk is framed, as to how it could be useful for different organizations, is that if an organization may have already aligned their security program to the Cybersecurity Framework or to the HIPAA Security Rule, this tool may be helpful for them to be able to identify potential gaps in their security programs if they are a HIPAA community. Maybe there are areas of HIPAA compliance that, by following the Framework solely, they maybe didn't account for. Or to bolster their security program, looking at the Crosswalk, as far as from the HIPAA Security Rule compliance in their existing program, aligning that existing program to the Framework and there may be some additional opportunities to improve the organization's security posture. Next slide, please.

And just as an example, I just pulled out one of the areas in the Crosswalk which builds upon some of the information that's already existing in the Framework. So, this example talks about the category of risk management strategy. And I just pulled out a couple of the subcategories related to risk management and this just kind of shows some of the components of the Crosswalk to the Security Rule whereby, in an example such as this, the Framework is more granular. So, there are more specific risk management subcategories that map or would map into the more general HIPAA Security Rule risk management implementation specification.

And there are other examples of this. For example, the Framework's subcategories regarding training are also more granular. There are subcategories regarding training for senior executives, for privileged users, for other users, and the standard for training in the HIPAA Security Rule doesn't go into that granularity. So, the Crosswalk would show the overall training and awareness standard and those resultant implementation specifications aligning with those more granular subcategories. And sometimes it works the other way. There may be a particular subcategory that may touch upon multiple HIPAA standards and implementation specifications and that would be reflected as well within the Crosswalk itself. Next slide, please.

As far as some of the cybersecurity guidance that OCR offers on our website, something that's relatively new, within the past maybe nine months or so, is we have rearranged some of our website to include a cybersecurity-specific landing page, where we include more cybersecurity-specific resources. Some of those resources include the ransomware guidance and the cybersecurity incidents checklist and accompanying infographic, as far as recommendations for entities for what to do if they encounter a cyberattack, including some resources and guidance about determining if a particular incident may raise to the level of a breach and what to do in those different instances. As well as our cybersecurity newsletters.

These are newsletters that generally come out about every month and they concern different cybersecurity topics. And because they are being published by the Office of Civil Rights, there is certainly an effort to, as some of these security topics more generally are discussed, discuss how they intersect with the HIPAA Security Rule. So, some examples of the newsletters that are out there: the difference between a risk analysis and a gap analysis; workstation security; software vulnerabilities and patching; disposing of electronic devices and media; securing electronic devices and media; and more of a general cyber hygiene and awareness for October for National Cybersecurity Awareness Month. Next slide, please.

One of the more recent things that OCR has collaborated on with ONC – ONC has the Security Risk Assessment Tool. So, there have been some revisions to that that were released just prior to the OCR/NIST conference and during the OCR/NIST conference, ONC and OCR conducted a briefing on the revised Security Risk Assessment Tool. So, some of the things that the tool is designed to do is primary to health, small and medium-sized entities, to help them identify the risks and vulnerabilities they have within their environments.

And the tool was updated to provide an enhanced functionality and documentation capabilities. There are methods by which organizations can upload documents into the tool itself to provide additional information, as far as what the entity is doing as far as implementing or assessing already implemented security controls as part of their risk assessment process, and to also provide demonstrations. Or if they just need, frankly, more space for more complex organizations than may be available in the comment boxes in the tool itself, to go into additional detail to help meet the requirements to provide the entities an opportunity to discuss different risk areas in an accurate and fair way as the Security Rule requires. The current revised Security Rule is available currently for Windows operating systems. The revisions were not applied to the prior Security Risk Assessment Tool iOS version but the older iOS version tool is still available on the Apple App Store. So, that is still an option for entities although, again, that has not been revised as of yet. Next slide, please.

Again, just some bullet points on some of the revisions that were incorporated into the new version: the user interface itself has been enhanced; the workflow process and how the different questionnaires and questions and guidance materials branch out among the different topic areas; the logic that goes into the assessment algorithm, as far as how that risk is calculated given the inputs of the entity choosing their own likelihood and impact scores for their different threats and vulnerabilities; progress tracking throughout the tool – you can certainly stop the tool because it can get a little lengthy at times and save your progress and come back to it; some of those improved threats and vulnerabilities; the final reports that are available to the user based on its inputs; tracking for integrating or inputting different assets and business associates and vendor information; and just an overall improvement of the user experience. Next slide, please.

So, the approach that was used for these revisions for the tool – we were engaged with a contractor – was a comprehensive usability testing of the original or Version 2.0 of the tool, with various users, healthcare practice managers, to get an assessment of some of the shortcomings of that version of the tool and get some feedback for what could be useful for people that actually use the tool to make it more functional, more useable, and more useful overall to the organizations that are going to make use of this information in the tool itself. So, that information that was conducted over that year period was incorporated into the revisions and development of the overall user experience of the tool, as well as the content of the tool itself.

There was testing done of the tool with the selected healthcare practice management community to assess how the revisions were going to be received within a broader community. And as the tool is now available on the HealthIT.gov website, there are opportunities to provide feedback to the tool and we certainly have encouraged that feedback of our user community and have talked about that during our briefing at the OCR/NIST conference. And we hope to examine that feedback and, where there are opportunities to provide additional enhancements to the tool based on that feedback from the user community, we would look and hope to be able to do so.

There is also an email there on this slide, privacyandsecurity@hhs.gov, which is another opportunity for people to provide feedback or if they need help using the tool itself due to technical issues. Next slide, please.

And this is just a brief rundown of the different sections of the tool that it guides you through: security risk assessment basics on doing the risk assessment process; an organization's policies, procedures, and documentation; workforce training and security overall of an organization, workforce management; some technical security issues and securing your data; physical safeguards; business associates and vendors; and contingency planning. So, these are the seven main sections that comprise the overall tool itself and how it goes about collecting and assessing information provided for assessing risk areas. Next slide, please.

So, these are just a couple of examples of some of the slides. This particular one is the welcome slide that is going to provide the user with a disclaimer, just making clear that no information that is going to be entered into the tool, or that the organization is otherwise going to use the tool for, is going to be transmitted to HHS. We want to make clear that HHS does not have any visibility into what users do with the tool. Any data that is created or entered into the tool is strictly going to remain local on the user's computer. After this main screen, the user is going to have opportunities to enter the username of the person actually going through the tool. They're going to be able to identify the practice information and begin using the tool itself. Next slide, please.

So, this is the next slide that's just going to provide an overview of the tool and provide information on the core steps that are included in the tool. On the left-hand side is a navigation pane that users can use to always go back to the home screen to go back to information about the practice or organization itself, as well as different assessment areas, summary, and an opportunity to save and quit the tool. Next slide, please.

And these are just, again, some example slides. And this particular one is just looking at some screenshots talking about the practice information, opportunities to enter data on facility locations, business associate information, asset information, and whatnot. Next slide, please.

And this is an example screenshot of what it would look like when an entity is given the opportunity to identify the likelihood of impact to different threats and vulnerabilities to their practice, which was based on some prior questions. One of the things that I really like about the tool is that when the users do go through the questionnaire part, based on what answer that they may give to a particular question area, there is an education box that will provide information about best practices or opportunities for improvement if an organization chooses a low level of protection for a particular questionnaire area. Next slide, please.

And, again, this is another screenshot. This is looking at some section summary areas that are going to indicate some areas of success for the organization, areas that the organization may want to consider having some additional review, some higher risk identification areas, to look at some enhancements to their existing security controls or whatnot. Next slide, please.

And this is going to be a summary dashboard, which is going to indicate the risk status and completion of the overall tool itself, as to where the organization is in different areas as far as risk scores and areas that are still awaiting review of the identity and identified vulnerabilities and whatnot. Next slide, please.

And those were a representative sample of some of the cybersecurity resources that OCR has available, both individually as OCR on our website and in our cybersecurity materials and also collaboratively with ONC with respect to revising the ONC Risk Assessment Tool, as well as with ONC and NIST in areas such as the Cybersecurity to HIPAA Security Rule crosswalk.

Aaron Miri – Imprivata – Co-Chair

Excellent. Thank you very much, Nicholas. I know we are running very, very short on time here so I don't know if we're going to have a lot of time to take a lot of questions. But I just want to say to you, as a healthcare provider/CIO, I have used your crosswalk, I have used a lot of your material, and I want to just appreciate the OCR for really engaging the healthcare community, the provider community, and really trying to help us and partner with us in moving the ball forward. So, I really appreciate that very much.

Nicholas P. Heesters, Jr. – United States Department of Health and Human Services Office for Civil Rights – Health Information Privacy Security Specialist

Thank you.

Aaron Miri – Imprivata – Co-Chair

Okay. So, I think we have time for maybe one question and then we have to move on, as appropriate to time, so we can keep this going. Anybody from the committee want to ask OCR any questions? I'll start with just one. One question that we've wrestled with, Nicholas, is I would say there are some challenges when it comes to state by state and some of the regulations, especially around privacy disclosure and breach notification and so forth and so on. Some states have really gotten aggressive with it. Some states conform to the national standard. One of the things we have talked about is the need for harmonization of those that would allow for providers, such as myself, to be able to know what is required and make sure that we meet each of those obligations appropriately. Is that a prioritization that you think we should continue to look at and talk about or is that not such a concern?

Nicholas P. Heesters, Jr. – United States Department of Health and Human Services Office for Civil Rights – Health Information Privacy Security Specialist

I certainly can appreciate the issues that you face with the multitude of state breach laws and how they impact organizations, especially healthcare organizations. Some state laws may, for HIPAA communities and those covered HIPAA, defer to their HIPAA obligations and then go into specific state obligations if they are not covered under a regulatory structure such as that. Other states may do their own thing regardless. So, it is a patchwork and I can certainly appreciate those issues and those concerns. To the extent that OCR can provide any help to this body or elsewhere for other information, I'm sure we'd be happy to do so. Other than acknowledging that this patchwork does exist and it presents problems for entities, we are kind of constrained by the statutory obligations in the HITECH Act that did create the HIPAA de-identification rule and our current environment.

Aaron Miri – Imprivata – Co-Chair

Got it. Thank you very much. I appreciate that. Okay. So, I know that we are close. Lauren, do we need to move to next phase now of this?

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Sorry, I was on mute. So, I think we did have just one quick agenda item to prep for the next meeting but actually the next full HITAC meeting has now been cancelled or rescheduled for next month. So, I think with that, we can probably start to wrap up unless there are any other perhaps outstanding questions or afterthoughts from one of our first two presenters.

Carolyn Peterson – Individual – Co-Chair

This is Carolyn. I just wanted to thank our presenters today for coming and providing us with this information. I know I have looked at these various things at different points in the past but it's a really helpful summary, bringing things together in one place, and a great roadmap for me of things to review as we go forward with the writing and the revisions on this draft and take it to the full HITAC. So, thank you so much for helping us to kind of realign our minds with all the things that can help us do the best job we need to do.

Aaron Miri – Imprivata – Co-Chair

And I second that.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Yes. Again, I want to thank our guest presenters today. This was a very informative call. We will now turn to public comments and if there's any additional remaining time, we can wrap up any outstanding items. SO, with that, operator, can you please open the public line.

<u>Operator</u>

Certainly, if you'd like to make a public comment, please press "*1" on your telephone keypad. A confirmation tone will indicate your line is in the queue and you may press "*2" if you'd like to remove your comment from the queue. For participants using speaker equipment, it may be necessary to pick up your handset before pressing the star keys. Again, that is "*1" if you'd like to make a comment at this time.

<u>Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer</u>

Great. Great. So, while we're waiting for any public comments to dial in, I just wanted to check in with our co-chairs. Since we are not going to have a full HITAC meeting next week, we likely will not have an opportunity to present to the full committee until about a month from now. So, I just wanted to see if there's anything that you think we should adjust in terms of our existing recommendations or thoughts. Maybe we can just touch on that point before we wrap up. So, let me just check in and see. Operator, do we have anyone dialing into the phone at this time?

<u>Operator</u>

Not at this time.

<u>Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer</u>

Okay. All right. So, I'll turn it back to the co-chairs and maybe we can spend our last five minutes just addressing if there's any outstanding items relative to our recommendations/report.

<u>Carolyn Peterson – Individual – Co-Chair</u>

Thanks, Lauren. I think it's important that we, if we can't do it in the next four minutes, that we as a workgroup review the recommendations and where we're at with that so far and kind of assess if there are other things that we need, other things that we think need further discussion in light of the information we received this morning. Certainly, what we've had today broadens the thinking around the issues and perhaps the direction we take. And that's all to the good. We should make sure everything is in alignment. Thoughts from anyone in the committee?

<u>Aaron Miri – Imprivata – Co-Chair</u>

Carolyn, this is Aaron. I echo that and I would also say that I really think today's speakers did an excellent job, articulating different dimensions of the way to sort of frame up some of the concerns that we've talked about generally, real-life circumstance stories that we know about, things we've experienced, and whatnot. So, I think it would behoove all of us to take some time to look at the materials from our speakers, think about the topic today, and see if there's any that synthesizes any of the questions that we want to think through. But I would agree with you, Carolyn.

Brett Oliver – Baptist Health – Annual Report WG Member

Yeah, this is Brett. If I could comment. These are fabulous resources and, for me, in some of these areas, it's like drinking from the firehose, just trying to stay afloat. It made me wonder if one of our recommendations may be to survey the landscape of end users as to their knowledge. I mean, I know we could look at – each of these individual groups could look at their utilization rate and folks accessing that. But have we set up this "if we build it, report it, post it, they will come" kind of setup? What's the general awareness for all these fabulous resources? And I know my security folks are going to have been aware of a lot of this stuff that we talked about today but we're one organization of moderate size. What about the individual group? What about the larger groups? Are they aware of these things? And I'm asking out of ignorance and perhaps that could be a recommendation that we survey to see what the general awareness of all these great resources is.

Aaron Miri – Imprivata – Co-Chair

This is Aaron. I can speak from experience. You're exactly right. The smaller, single providers, they don't have the resources and the ability to look at all this. I think they are trying and doing a good job and the market is evolving. And we, as large health systems – yourself, Brett, myself, others – we have the resources to stay engaged and really be thorough but for the individual, little guy out there, it's very difficult. So, I would agree with you. It would be interesting to see what the disparity is. Is that a gap that we can help address with just reinforcing all this great material that's out there?

Carolyn Peterson – Individual – Co-Chair

Any additional thoughts, Christina or Chesley?

Christina Caraballo – Get Real Health – Annual Report WG Member

Yeah, this is Christina. I would just chime in and say that these are excellent presentations, very rich in information. As just a task for us, I think we should look at our recommendations around privacy and security so far and see if we want to make any adjustments based on these presentations and also considering future work for HITAC. So, just revisiting that and I think that, Aaron, you mentioned that as well. So, I'm agreeing with you there. That sounds like a good approach.

Chesley Richards – Centers for Disease Control and Prevention – Annual Report WG Member

And this is Chesley. I would second that.

Carolyn Peterson – Individual – Co-Chair

Okay. Thank you. I can't think of anything else that I have on the radar. Do you have anything else, Aaron?

Aaron Miri – Imprivata – Co-Chair

No. I think we are right on the money. And I just really appreciate everybody. This is excellent. Excellent discussion.

Carolyn Peterson – Individual – Co-Chair

Agreed.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Okay. Thanks, everyone, for your time today. Thanks to the workgroup members and thanks again to our special guests. Again, we always post our workgroup meetings on healthit.gov.

Aaron Miri – Imprivata – Co-Chair

Thank you.

Carolyn Peterson – Individual – Co-Chair

Thank you.

Lauren Richie – Office of the National Coordinator for Health Information Technology - Designated Federal Officer

Bye, everyone. Thanks.

Brett Oliver – Baptist Health – Annual Report WG Member

Have a good weekend, everyone.

Carolyn Peterson – Individual – Co-Chair

Thank you.

Brett Oliver – Baptist Health – Annual Report WG Member

Bye-bye.