National Committee on Vital and Health Statistics

Transcript

July 20, 2022 10:30 a.m. – 4:30 p.m. ET

Virtual

SPEAKERS

NCVHS Members		
Jacki Monson	**Sutter Health**	**Chair**
Sharon Arnold	**DHHS**	**Executive Staff Director**
Rebecca Hines	**NCHS**	**Executive Secretary**
Debra Strickland	Conduent	Member
Denise E. Love	Individual	Member
Jamie Ferguson	Kaiser Permanente	Member
Margaret A. Skurka	Indiana University Northwest and Principal, MAS, Inc	Member
Melissa M. Goldstein	The George Washington University	Member
Richard W. Landen	Individual	Member
Tammy Banks	Individual	Member
Valerie Watzlaf	University of Pittsburgh	Member
Vickie M. Mays	UCLA	Member
Wu Xu	University of Utah	Member
Maya Bernstein	ASPE/OSDP	Staff
Lorraine Doo	CMS	Staff
Natalie Gonzales	CDC	Staff
Marietta Squire	NCHS	Staff
Susan Jenkins	ASPE	Staff
Grace Singson	ASPE	Staff
Greg Garcia	Health Sector Coordinating Council	Executive Director, Cybersecurity

Andrea Matwyshyn	Pennsylvania State University	Professor of Law and Engineering Policy
L. Reuven Pasternak	National Risk Management Center, Cybersecurity and Infrastructure Security Agency	Senior Advisor
Linda Ricci	Food and Drug Administration	Director, Division of All Hazard Response, Science and Strategic Partnerships

Call to Order/Roll Call

Rebecca Hines: Good morning and a warm welcome to our members of the National Committee on Vital and Health Statistics, NCVHS, and welcome to committee staff and members of the public in attendance with us today. This is our summer or mid-year meeting of the committee. My name is Rebecca Hines and I serve as Executive Secretary and Designated Federal Officer for NCVHS.

With the ongoing situation with COVID, we continue to meet virtually. I know a number of you have asked and we anticipate doing so for the remaining meetings of this year. We are in the process of scheduling the third 2022 meeting of the Full Committee for some time either in November or early December. The Standards Subcommittee also is working on scheduling a one-day listening session as you will hear this morning. You can visit the committee website and if you have not already, you can sign up to receive email notices from us. You can visit the home page of the NCVHS website to do that. It is NCVHS.hhs.gov. Perhaps, Marietta, you can put that in the chat to all participants.

Let us take care of roll call now. Please state your name, your status as a special government employee, and any potential conflicts with today's work. Starting off with our chair, Jacki.

Jacki Monson: Good morning. Jacki Monson, Sutter Health, Chair of NCVHS, no conflicts.

Rebecca Hines: Thank you, Jacki.

Deb.

Debra Strickland: Hi. Deb Strickland, member of the Full Committee and member of the Standards Subcommittee. No conflicts.

Rebecca Hines: Denise.

Denise Love: Denise Love, independent consultant. I am a member of the Full Committee and Co-Chair of the Standards Subcommittee. No conflicts.

Rebecca Hines: Thank you. And for the record, Denise Chrysler is unable to be with us today.

Jamie.

Jamie Ferguson: Good morning. I am Jamie Ferguson. I work for Kaiser Permanente. I am a member of the Full Committee and Subcommittee on Standards and I have no conflicts.

Rebecca Hines: Margaret.

Margaret Skurka: My name is Margaret Skurka. I am Professor Emerita at Indiana University. I am a member of the Full Committee and I serve on the Subcommittee on Standards, and I have no conflicts.

Rebecca Hines: Melissa.

Melissa Goldstein: Hi. I am Melissa Goldstein. I am a professor at George Washington University. I am a member of the Full Committee, Co-Chair of the Privacy, Confidentiality, and Security Subcommittee and I have no conflicts.

Rebecca Hines: Rich.

Rich Landen: Good morning. Rich Landen, member of the Full Committee, member of the Executive Subcommittee, Co-Chair of the Standards Subcommittee. I have no conflicts.

Rebecca Hines: Tammy.

Tammy Banks: Good morning. Tammy Banks, member of the Full Committee, member of the Subcommittee on Standards and no conflicts. Thank you.

Rebecca Hines: Val.

Valerie Watzlaf: Good morning. I am Val Watzlaf. I am an associate professor emerita with the University of Pittsburgh. I am a member of the Full Committee, and I am also serving as Co-Chair of the Subcommittee on Privacy, Confidentiality, and Security. I have no conflicts.

Rebecca Hines: Vickie.

Vickie Mays: Good morning, everyone. I am a professor at the University of California Los Angeles. I am a member of the Full Committee. I Co-Chair our workgroup and I am member of the Subcommittee on Privacy, Confidentiality, and Security and I do not have any conflicts.

Rebecca Hines: And last, Wu.

Wu Xu: Good morning. My name is Wu Xu. I am with the University of Utah, a member of the Full Committee. I have no conflicts.

Rebecca Hines: We have a quorum. Just a note on the agenda. For both today and tomorrow, we are including a public comment period. Today's is scheduled for 4 p.m. For members of the public at that time, you are welcome to make a comment orally. We will provide instructions. They are actually showing here now as well. You can see that you can send a written comment to the NCVHS mailbox posted here on the slide. NCVHSmail@CDC.gov. We will read your comment for the committee to hear if you prefer to comment that way rather than orally live. It is possible that the public comment could fall a few minutes earlier than 4 o'clock or later, depending on how the session right before goes. Just note that. It is just something to be aware of. I am going to put in the chat for those who may not have it, the agenda for today.

With that, I think we can turn it over to our chair for a review of the agenda.

Agenda Review

Jacki Monson: The plan for today. We have a very robust agenda and some exciting topics to discuss with everyone. The plan is to get an ASPE update from Sharon Arnold. We will then move into Subcommittee on Standards with Rich and Denise covering the Convergence 2.0 Project as well as we have an action there, a letter for recommendations on modernizing and adoption of HIPAA transaction standards.

We will take a break and then we will go back to the Subcommittee on Standards for additional updates. They are going to provide a status on the new HIPAA transaction standards and operating rules and developments and ICD-11 transition.

Then we will move into the Subcommittee on Privacy, Confidentiality, and Security, a briefing on current issues in cybersecurity. When that concludes around 4:00 p.m., we will have public comment, open it up for a Full Committee discussion and then we will wrap and adjourn for the day.

Without further ado, let us start with an update from Sharon.

Rebecca Hines: You know what. I forgot to introduce staff. I apologize. Let us begin. I am sorry, Sharon. Starting with you.

Sharon Arnold: Hi. I am Sharon Arnold. I am the Executive Director of the National Committee on Vital and Health Statistics. I am also the Associate Deputy Assistant Secretary for Science and Data Policy in the Office of the Assistant Secretary for Planning and Evaluation.

Rebecca Hines: Thank you. And Susan Jenkins.

Susan Jenkins: I am Susan Jenkins. I am in the office in which Sharon is. I am the division director for the Division of Evidence, Evaluation, and Data Policy. I am happy to be here today.

Rebecca Hines: Maya Bernstein.

Maya Bernstein: Good morning, everyone. I am Maya Bernstein. I am the Senior Advisor for Privacy Policy at ASPE. I work for Susan Jenkins and Sharon Arnold. I am also the Lead Staff to Sharon in her role as the Executive Director of this Committee and at the moment, Lead Staff of the Subcommittee on Privacy, Confidentiality, and Security.

Rebecca Hines: Thank you, Maya. We have our newest addition to ASPE, Grace Singson. Grace, did you want to say good morning.

Grace Singson: Good morning, everyone. My name is Grace Singson. I am an ORISE Fellow. I am supporting the SOGI and SDOH Workgroup. I am with Maya, Susan, and Sharon.

Rebecca Hines: Thank you, Grace. Lorraine Doo, the Lead Staff to Standards, is with us. She will be in another call for the next couple of minutes and then she will be on. I think that is what caused my confusion there. With that, Sharon, the floor is yours.

ASPE Update

Sharon Arnold: Wonderful. I am very delighted to be here with you. Although we are meeting now virtually, I am happy to report that we are considering whether to meet all together in Washington at meetings next year. I hope that we will be able to meet in person soon.

The committee did hold an abbreviated meeting in March. I did not address you then. A lot has happened since I have talked to you in January. When I last spoke to you, we were experiencing a peak in the Delta Variant of the COVID virus. Only the political leadership and a few executives have returned to the office. The full-on return originally planned for early in the year was delayed due on variants emergence. Of course, our headquarters in the Humphrey Building has been open 24/7 since March 2020. We never closed. In particular, the Uniformed Public Health Service, who we call the Commissioned Corps, are always in the building, running the Secretary's operation center and carrying out public health activities related to the pandemic, the refugee situation on the southern border, and other duties that cannot be carried out effectively remotely.

However, significant portion of our workforce continues to telework most of the time. The workplace operates much differently than it did three years ago and we are still adjusting to a new hyperlink doing things – upgrades to our technology infrastructure.

Given all of that, I am really proud to share that the department ranked number two in the most recent results of the Federal Employee Viewpoint Survey or FEVS, which is an annual survey of federal employees, representing the most comprehensive analysis of federal workforce engagement and satisfaction. HHS was second only in NASA among large agencies. Of course, NASA is really hard to beat. They have the coolest mission in government. But we really feel like our ranking is something to brag about.

We continue to rely on the science and the best available public health information, including guidance from the CDC to plan both our workforce policies and health care and public health policies that affect the nation. In the meantime, the regular cadence of work of the department continues along with the number of high priorities.

In January, it was hard to imagine there could be a development in health communities that could compete with the COVID pandemic. But following the mass shootings in Buffalo, New York and Uvalde, Texas just five days apart and then the Supreme Court's decision in Dobbs v. Jackson Women's Health Organization, then safety and reproductive health rose to more prominence among the Secretary's priorities.

Recognizing that many people hold strong views about these issues, I am just going to summarize actions the department has taken in response to these national events. Many of these support and extend the Secretary's commitment to strengthen mental health that the President announced in the State of the Union Address in March and I will talk more about that in a moment.

On May 27, multiple operating divisions of the department responded to the needs of the communities in New York and Texas affected by gun violence. These actions will also support Illinois where residents of Highland Park experienced another mass shooting on July 4. These activities include disaster services and crisis counseling, technical packages developed by CDC to help states and communities take advantage of the best available evidence to prevent violence and increase focus on mental health, which I will describe later.

In anticipation of the Supreme Court actions in January, the Secretary established HHS Interagency Task Force on Reproductive Health Care Access. This Task Force includes subject matter experts across the department and its primary goal is to facilitate collaborative, innovative, transparent, innovative, and action-oriented approaches to protect and bolster sexual and reproductive health. The Assistant Secretary for Health, Admiral Rachel Levine, and our Assistant Secretary for Global Affairs, Ms. Loyce Pace, served as the co-chairs of this coordinating body.

Following the Supreme Court's decision in Dobbs, Secretary Becerra announced HHS' action plan to protect access to reproductive health care, which includes the following six priorities. Increasing access to medication abortion, protect patients and providers from discrimination, ensuring privacy for patients and providers, protecting emergency abortion care, ensuring providers have family planning, training, and resources, and strengthening family planning care, including emergency contraceptive.

Since the plan was announced, HHS has taken the following actions. The department launched a reproductiverights.gov public awareness website, which includes Know Your Rights patient factsheet. Secretary Becerra and the Secretary of Labor, Marty Walsh, convened a meeting with health insurers and sent them a letter, calling on the industry to commit to provide coverage for contraceptive services at now cost as required by the Affordable Care Act.

The Office of Civil Rights published guidance to patients and providers that address the extent to which HIPAA protects individual's private medical information when it comes to seeking abortion and other forms of reproductive health care as well as when it comes to using health information apps on electronic devices.

The Office of Population Affairs announced nearly $3 million in new funding to bolster training and technical assistance for the nationwide network of Title X family planning provides.

Additionally, following the President's Executive Order of protecting access to reproductive health care services, HHS has issued guidance to clarify that emergency medical care includes abortion services. And HHS has also issued guidance to the nation's retail pharmacies, clarifying the obligations to ensure access to comprehensive reproductive health care services.

Despite these other high-profile issues, COVID continues to require significant attention and resources. On July 15, Secretary Becerra signed a tenth renewal of the declaration of a public health emergency for COVID-19. This supports multiple HHS efforts against the current pandemic.

CDC continues to provide updated information on COVID-19 cases, deaths, hospitalizations, vaccinations, and more on the website, COVID Data Tracker. The website is updated every weekday but no longer on weekends.

In March, CDC announced a change from relying on metrics associated with community transmission to a three-part metric called community levels. Community transmission refers to measures of the presence and the spread of the virus that causes COVID-19. Community levels refers to measures of the impact of COVID-19 in terms of strain, health care system, and hospitalizations while accounting for transmission in the community.

CDC continues to publish both COVID-19 community levels and community transmission, but now recommends the use of COVID-19 community levels to determine the impact of COVID-19 on communities and to take action.

The community-level metric uses three indicators. The new COVID-19 cases per 100,000 population in the last 7 days, new COVID-19 hospital admissions per 100,000 in the last 7 days, and percent of staff inpatient beds occupied by patients with confirmed COVID-19, which is a seven-day average.

We are currently in a wave of the BA.5 omicron variant. About 75 percent counties are medium or high community levels and almost 93 percent of counties are classified as high transmission. COVID-19 community levels currently indicate that the impact of COVID-19 is increasing in many areas of the

United States. Importantly, the case rates, which are included in both the transmission levels and the community levels are currently underreported because of the emergence of home testing.

CDC continues to promote the National Wastewater Surveillance System to health departments to partner with CDC laboratories and local wastewater utilities to get high-quality, community-level data. Currently, there are over 1000 testing sites across the country. Around 42 percent of sites are currently seeing some of the highest levels for those sites since December of 2021. About 36 percent of all sites reporting wastewater data are experiencing a decrease in SARS-CoV-2 levels and about 54 percent are reporting an increase.

On March 29, 2022, the Advisory Committee on Immunization Practices recommended a second COVID-19 booster dose for adults aged 50 years and older and for persons with moderate to severe immunocompromise. CDC's COVID data tracker shows that in total, 48.1 percent of people over the age of 5 are fully vaccinated. 19.3 million people have received their second booster but only 28 percent of those 50 years and older have received the second booster.

On June 17, we passed a milestone many parents were eagerly awaiting. FDA's Emergency Use Authorization for the use of Moderna and Pfizer COVID-19 vaccine for children down to six months of age. A month later, about 400,000 children under the age of 5 have gotten their first dose.

Earlier this month on July 6, FDA revised the Emergency Use Authorization for the anti-viral Paxlovid, allowing licensed pharmacists to prescribe Paxlovid to eligible patients, thereby, increasing patient access to treatment and reducing the burden on the primary care system.

Last week on July 13, the FDA issued an Emergency Use Authorization for the protein-based Novavax COVID-19 vaccine. That is for the prevention of COVID-19 in individuals 18 years of age and older. Authorizing an additional vaccine expand the available vaccine options for the prevention of COVID, including the most severe outcomes that occur such as hospitalization and death. This vaccine offers an option to individuals who may be allergic to a component in mRNA vaccines or have a personal preference for receiving vaccines other than mRNA-based vaccines.

ASPE has published seven articles on COVID in 2022, including two documents on vaccine hesitancy of parents and a claims data analysis estimating hospitalization cost savings of $2.6 billion due to vaccinations among Medicare beneficiaries.

ASPE also published a scoping review identifying SDOH data elements that maybe associated with higher risk of COVID-19 infections and analysis of the quality of COVID-19 data collected on major federal platforms.

Despite our focus on COVID, HHS continues to pay close attention to other emerging contagious diseases. The number of reported worldwide measles cases increased by 79 percent in the first two months of 2022 compared to the same time last year.

The UN UNICEF reports that pandemic-related disruptions increasing inequalities and access to vaccines and the diversion of resources from routine immunizations are leading too many children without protection against measles and other vaccine preventable diseases. The risk for large outbreaks of measles has increased as communities relax distance and practices and other preventative measures for COVID-19 implemented during the height of the pandemic.

In addition, with millions of people being displaced due to conflicts and crises, including Ukraine, Ethiopia, Somalia, and Afghanistan, disruptions in routine immunizations and COVID-19 vaccination service, lack of clean water and sanitation, and overcrowding increased the risk of vaccine preventable disease outbreaks.

Through the Health Alert Network and push and outreach and communication activity calls, the CDC has identified at least 1,972 cases of monkeypox in 46 states with New York having at least 500 cases.

Prior to the current outbreak, CDC conducted testing of monkeypox inhouse. However, the rapid spread of the virus prompted the CDC to expand testing capacity by partnering with five commercial laboratories to carry out testing.

Supporting the Biden's Administration's comprehensive strategy against monkeypox, HHS ordered 5 million doses of the two-dose vaccine, offering protection against both smallpox and monkeypox, which is approved for adults 18 and older.

There are a lot of other activities that have been going on. President Biden recently proposed a creation of the Advanced Research Projects Agency for Health or ARPA-H, to improve the US Government's ability to speed biomedical and health research and on March 15, he signed legislation authorizing the establishment of ARPA-H as an independent entity in HHS.

Secretary Becerra appointed Adam Russell to serve as the Acting Deputy Director of ARPA-H. In this role, Russell will lead the intensive process to stand up ARPA-H by continuing to build the infrastructure, business processes, and policies, which could take up to a year. The mission of ARPA-H will be to make pivotal investments in breakthrough technologies and broadly applicable platforms, capabilities, resources, and solutions that have the potential to transform important areas of medicine and health for the benefit of all patients and that cannot readily be accomplished with traditional research or commercial activity.

Supporting President Biden's Executive Order on tackling the climate crisis at home and abroad, HHS established the Office of Environmental Justice on May 31. The office represents HHS on the Federal Interagency Working Group on Environmental Justice and houses the HHS Environmental Justice Working Group and HHS' work on the Justice40 Initiative.

Justice40 is the administration's initiative to ensure that federal agencies deliver 40 percent of the overall benefits of climate, clean energy, affordable and sustainable housing, clean water, and other investments to disadvantaged communities.

In total, hundreds of federal programs representing billions of dollars in an annual investment are being utilized to maximize benefits to disadvantaged communities through the Justice40 Initiative.

After starting implementation on two Justice40 pilot programs, HHS is proud to prioritize three programs to include in the Justice40 Initiative that will help communities find relief from pollution and climate-related events impacting people's health.

In order to combat the infant formula shortage crisis under Operation Fly Formula, the Department of Health and Human Services is partnering with the US Department of Agriculture and with General Services Administration to import infant formula from other nations that meet US health and safety standards so that formula can get to store shelves faster.

Infant Fly Formula Flights will have completed 48 flights and imported more than 55 million 8-ounce bottle equivalence of infant formula. In addition, on May 18, President Biden issued a memorandum that delegated a Defense Production Act priorities and allocation authorities to the Secretary with respect to infant formula to address the shortage in the United States.

Now, I turn to mental health. In President Biden's First State of the Union, he laid out the administration's strategy to address the national mental health crisis to strengthen system capacity, connection to care, and to create a supported environment. This whole of government strategy will directly impact one of the Surgeon General's top priority's workforce programs. A surgeon general's activity advisory published this year was a call to action to address health worker burnout, which was seen between 35 and 54 of the nursing workforce. The 2022 Medscape report on physician burnout and depression sounded the same alarm on the results of their survey indicated that one out of ten physicians had suicidal ideation.

This month, the US made a transition from the ten-digit National Suicide Prevention Lifeline to 988, an easy to remember three-digit number for 24/7 crisis care. This lifeline, which also links to the Veterans Crisis Line, follows a three-year joint effort by HHS, the Federal Communications Commission, and Veterans Affairs for crisis care more in reach for people in need.

Secretary Becerra has renewed the determination of a public health emergency regarding the opioid crisis that was first declared in October of 2017. As of the beginning of this month, we have a clearer picture of total drug overdose deaths that occurred in 2021. There were an estimated 107,622 drug overdose deaths in the United States during 2021, an increase of nearly 15 percent from 2020. But the 2021 increase was half of what it was a year ago when overdose deaths were 30 percent from 2019 to 2020.

HHS has been working hard on coordinating an overdose prevention strategy. There was a recent release of a CDC clinical practice guideline for prescribing opioids for chronic pain. The draft guideline was published in the Federal Register for 60-day public comment that closed in April and the guidelines would update and expand the CDC guideline for prescribing opioids for chronic pain and provides evidence-based recommendations for clinicians who provide pain care.

In fiscal year 2023, a total of $21 billion is allocated for evidence-based treatment programs for opioid use disorders. This includes HRSA's announcement last month of the availability of $10 million in grant funding to increase access to substance misuse treatment in rural areas.

HHS also announced $1.5 billion in funding available through SAMHSA for state opioid response, $55 million in tribal opioid response and $44 million for mental health and substance use services for people who are at risk or are living with HIV/AIDS.

We had several new appointments in HHS. In February, Dr. Bob Califf was sworn in as Commissioner of the Food and Drug Administration. Robert Valdez was named as the Director of AHRQ and Bob Leavitt as the Deputy Assistant Secretary of Human Resources and Chief of Human Capital of HHS.

And also, closer to home, the President nominated Dr. Rebecca Haffajee, who has the Principal Deputy Assistant Secretary of ASPE to be the Assistant Secretary for Planning and Evaluation. That is my boss. The Senate Finance Committee, which has jurisdiction over health matters, gave her a hearing last week and we eagerly await her confirmation.

The 2022 to 2026 HHS Strategic Plan was published this spring. The Strategic Plan consists of five strategic goals for HHS: protect and strengthen equitable access to high-quality and affordable health care, safeguard and improve national and global health conditions and outcomes, strengthen sexual well-being, equity, and economic resilience, restore trust and accelerate advancements in science and research for all, advance strategic management to build trust, transparency, and accountability. In support of the strategic plan and in accordance with the Evidence Act, ASPE also published the HHS evidence building plan, the HHS capacity assessment, and the HHS evaluation plan.

ASPE also serves as the federal coordinator for the Interagency Task Force on Combating Antibiotic-Resistant Bacteria or CARB, which is implementing a national action plan to improve infection prevention and control of antibiotic stewardship, enhance surveillance of resistant pathogens and foster innovation in diagnostics treatment and vaccines, and to work with global partners.

ASPE also works to support innovation through policy research to better understand challenges, to developing new antibiotic products, and formulating options to invent the development of new antibiotics, which is needed as older products become less effective.

The task force recently published a report highlighting progress made since the carbon issue was launched in 2015, including more than doubling the number of hospitals with high-quality antibiotic stewardship programs, bringing relevant animal antimicrobial drugs under veterinary oversight and supporting research to better understand, prevent, and treat resistant infections. This is just a highlight of the important activities we have been undertaking since I last reported to you. And I am very happy to take any questions you have.

Rebecca Hines: Vickie.

Vickie Mays: That was an incredible report. It is like wow. How much has been going on. It is intense. I want to thank you for such a great report.

I am going to focus my questions and comments on as probably everybody would expect, on the mental health announcements that you made. I hope I am not getting too much in the weeds on this. But one of the things I want to ask is – I was really excited to hear – we all have been awaiting 988 and we want to see how it works. I guess I want to know two things about 988 and that is who does this fall under and are we collecting data to understand who we might be missing in 988.

And then my other mental health question has to do with we have a lot of cutbacks years ago in mental health data that were in the NCHS health surveys. We kind of booted it to SAMHSA. Many of us really miss the relationship between mental health and health. We know what the mental health consequences are. But we are not following real well Americans around the health consequences. And particularly with COVID, this has risen as a very important issue. Is there any likelihood that resources will be put into having more mental health questions in health surveys?

Sharon Arnold: With respect to your first question about are they capturing information from 988, I do not know the answer to that, but I can certainly find out and report back.

I think that the department is very conscious of the need to collect more information on mental health and to link with other important variables. We have been working through some of the issues on that. I think Maya has been providing an important service in efforts to think about how to link data while protecting privacy. Let me suffice it to say that it is a very complicated issue. There is a lot of activity, but we all recognize the importance of that. Maya, I do not know if you want to say a word or two about that.

Maya Bernstein: Sorry. I lost my file for a moment, and I missed the question.

Sharon Arnold: In the efforts to improve the linkage of mental health and health data.

Maya Bernstein: I can say a little bit about that. There was a requirement and law that we work to reconcile, if you will, the HIPAA privacy rules with the rules on what we call Part 2, 42 CFR Part 2, the substance use disorder treatment confidentiality rules. That effort is under way.

I think in the agency's public regulatory agenda, you will see that there is a listing there for an upcoming rulemaking. I cannot tell you the timing of that. But suffice it to say that the department is actively working on it. It is quite complex. There are a lot of moving parts about exactly how this would work.

I think we might see changes both to SAMHSA rules and to the HIPAA regulations at that time. We do not know yet how that will come out and exactly what will happen. But there is an effort under way. Is that responsive to what you were asking, Vickie?

Vickie Mays: Yes. With one more question. Is there the possibility of data being collected in the NCHS surveys that are on health because that then gives us a monitoring and surveillance and not necessarily just diagnosed disorders?

Maya Bernstein: I certainly cannot respond for NCHS. There may be another expert here from either Rebecca or one of her colleagues from NCHS who may be able to tell us that. I do not know what NCHS' plans are over at CDC.

Rebecca Hines: Happy to get back to you on that, Vickie.

Rich Landen: Sharon, thank you for such a comprehensive report. It reminds us just how complex this world is that we are dealing with. And since we, as NCVHS, deal with it in a thought leadership mode rather than an operational or program management way, it presents its challenges.

I also would like to comment on some of the mental health aspects and specifically, what we, the Standards Subcommittee, will be getting into later with its Convergence 2.0 project recommendations, is all about how we take HIPAA since HIPAA is a specific charge of NCVHS, the administrative and transaction set specifically, how we look at that in a world of convergence with the clinical standards and the pandemic and now 988 and how globally information tracks with the patient in an appropriate, meaning within the regulations, within privacy, confidentiality, and security, how that moves around and that indeed was one of the sets of issues that the subcommittee was wrestling with is that HIPAA both enabled some of that data flow and yet by structure, which because it is 25 years old, it also imposes some challenges, some barriers to the flow of that data. I hope later when we get to the recommendations and the discussions around the global picture of which these recommendations are a next step, not an end in and of itself, that the conversations and the information that ASPE has presented this morning can be folded into that discussion and help us make a truly global contribution to data flows that appropriately support services to patients. Thank you for that presentation.

Jacki Monson: Any other questions for Sharon?

Vickie Mays: Sharon, can you talk at all about in terms of COVID because the metric that you talked about that is used in this community whether or not they have improved the collection of race and ethnicity specifically in the hospitalization data. That was where we had the most problems in COVID. That metric is turning out to really be great in cities and states. But I do not know how the feds get cities and states to improve that and whether or not there was anything when that was developed to help improve that data collection.

Sharon Arnold: The data collection is an ongoing effort and challenge to encourage states and localities and hospitals to provide comprehensive data, including data on race and ethnicity. It is an ongoing challenge, and we continue to work on that is all I can say. We do not generate the data. Initially, we get it from our partners. We are continually providing technical assistance and efforts to prevent and trying to encourage that data producers to provide the very important data, race and ethnicity.

Denise Love: I wanted to follow up on Vickie's statement. Thank you for your update, Sharon. I think we are looking at the CDC – the current RFA or RPF out for state and local who are applying for public health infrastructure grants. There is a lot of hope that that will provide some infrastructure building, staff training, staff capacity so they can work with their submitting partners because the hospitals are not consistently trained as well. We are going to look to our public health partners to work with their local submitters to improve this race ethnicity data.

Also, in the session coming up, we will talk a little bit about social determinants data and trying to reduce the fragmentation of that throughout our whole system because it is an ongoing problem and it will be an ongoing effort to harmonize some of that data. I just wanted to acknowledge the CDC grants are providing some hope that there will be improved coding at the local level and collection.

Jacki Monson: Any other questions for Sharon?

Seeing no hands, Sharon, thanks so much for such a robust update this morning.

Melissa, do you have one last question?

Melissa Goldstein: I do. Sorry. I was slow on the raising the hand button. I was just wondering, and I am not sure whether this has progressed yet because obviously, it is a very new issue although we may have been expecting it for a few months at this point. Is the department considering changes to privacy rules to protect reproductive health and protective health information in any way that can be done in the absence of specific legislation from Congress? I am just wondering if there is anything that the department is considering now obviously on a public level that you can share with us.

Sharon Arnold: I think the department is looking at options and authorities. We will continue to look at ways that we can support reproductive health – any more than that. I cannot --

Melissa Goldstein: I certainly understand. Thank you very much for the comprehensive presentation. You guys are very busy. I appreciate that. Thanks very much.

Sharon Arnold: Thank you very much.

Jacki Monson: Let us move on to the next agenda item, which is standards. Denise and Rich, I will turn it over to you.

Subcommittee on Standards

Rich Landen: Thank you, Jacki. If we could bring up the Power Point presentation, please. Let me set the stage by saying that the recommendations that the Subcommittee will be presenting for discussion and hopefully approval by the Full Committee today, we substantively went over at our January meeting this year where all these concepts were still draft ideas. It is part of the ongoing project or series of projects that the Subcommittee has had for the last six or eight years around administration simplification transactions and code sets. What we are considering today is the next step, not the last step, not the final step of the process.

I want to express my appreciation particularly to all the Subcommittee members, who have been working, not just diligently, but over time and a half in putting all of this together since our listening session that we held back in June. And to the members of the Full Committee, I not exactly apologize but I regret we could not get this to you sooner. We had a couple of meetings with important federal partners specifically CMS, Office of Burden Reduction, Health Informatics, and the Office of the National Coordinator that only happened earlier this week. The good news coming out is we have lots of good comments and substantively nothing has changed. But the packaging, how we address, now we approach some of the recommendations and supporting materials. We had to scramble for the last 48 hours to consider the input we got from CMS and from ONC. As much as we would have liked to have gotten a final draft to you a week or two ago, you only got this this morning.

But as I said, the good news is the substance has not really changed from the June 9 materials that you saw and the substance was also covered fairly deeply at our January meeting. I am hoping that given an opportunity for questions, answers, and discussions, this will not be unfairly hitting you at the last moment.

With that in the way of introductions and apologies, let us take a look at what we will be talking about when we go through the letter and the recommendations for approval. As I mentioned, this is part of Convergence 2.0, which is as following. Built on the Predictability Roadmap. This is something the committee and the subcommittee had been working at for the past six or eight years. It is about the optimization of the data value specifically in the HIPAA world but joined at the hip with the standards process that affects the electronic health record that is in the charge of the Office of the National Coordinator. And then as you will see as we get into some of the detail, it also refers to other standards that are not really within either the CMS Office of Burden Reduction Health Informatics or ONC but yet still need to be somehow or another integrated into the system for data flows, irrespective of the legislative authorities for the regulations of those particular aspects of the standards or the programs.

These next two slides are simply a repeat. You saw this slide in January. These are the themes that emerged from another listening session, which was August of 2021, at which we elicited from industry. What are their top concerns? What are their priorities? What is it that needs to be done to achieve the goals of HIPAA and the optimization, the efficiencies, and the reliability of the systems that HIPAA put in place many years ago, in which have been substantively modified by additional pieces of federal legislation and by the regulatory experience?

Testing and evaluating standards and return on investment was key. Attachment transaction standard and acknowledged transaction standard. Prior authorization as we have discussed over the last three years in conjunction with ONC and HITECH is key. And improving regulatory process for adoption of standards and looking at the ONC standards advancement process for lessons learned. These were all key considerations.

Patient education particularly around the apps available to patients and privacy and security policies. Training programs for providers on data exchange in this world of bidirectional data exchange because providers especially as you get smaller in scale, there is less and less expertise and fewer and fewer resources available to educate the staff on the implications of what is happening in and around the data exchanges.

Identifying, implementing, and adopting standards for payers to exchange data bidirectionally. Again, referencing to HIPAA. The state of the art then was a claims transaction, originating to the provider from Point A, went to Point B, the payer, and that was pretty much the scope of the structure.

Today, we have much more conversational uses of the information the data contained in the transactions and those data in those transactions can go between more parties than just Point A to Point B. It is time to look at some of the structure there.

Number nine was patient matching. That is being addressed elsewhere particularly by ONC. That did not make it into our inclusions for today.

Item ten. Again, a key concept. Expanding the HIPAA concepts to non-covered entities to reflect the fact that the HIPAA protections, which apply only to covered entities and business associates really does not protect the data in respect to some of the routine uses of the data. Data captured under HIPAA, collected under HIPAA is subject to the HIPAA privacy and security constraints. But once it legitimately leaves that umbrella of covered entities, it no longer enjoys the protections. We have heard a lot on this in the past years from our sister subcommittee, Privacy, Confidentiality, and Security.

The foundation of these recommendations today – here is just a little bit more background. We sent three recommendations to HHS. In March of this year, we had a special meeting. Those were kind of general-purpose recommendations.

We have consistent themes. The key among them is e-commerce has changed since HIPAA in 1996. There are new types of standards and new technology that are in use by covered entities and their vendors, particularly for business practices that are burdensome.

Some components of the HIPAA framework are either outdated or dysfunctional. Objective and methodical evaluation is necessary to determine risks and define potential remediation options. An example of that. When HIPAA was first passed, the industry was concerned that the updates to the standards would be too frequent for industry to absorb. HIPAA essentially codified that updates shall be made no more frequently than annually. It was recognized that updates were critical.

But now as we look at history, since HIPAA was – since the first regulations were adopted under HIPAA, there has really only been one update. One update in 26 years is not the frequency that the framers envisioned back then. That lack of consistent updates to reflect new data new needs, new business models, new practices, new information requirements be they federal program or state initiated. The HIPAA framework is for whatever reason and there are lots of reasons, it is just not keeping up with the business needs. We need to do the updates more speedily.

Standards development processes, structure and service capabilities are not comparable. Different SDOs do things differently, which is fine. But that means we have some different outcomes and different ways of evaluating things. Best practices could be evaluated for broader use. And the specific example that – one specific example comes to mind are the conformance statements. X12 has a different charter and different set of expectations, different model. X12's implementation guides do not get into conformance a lot and hence the concept of the operating rules authoring entity and operating rules came into being.

NCPDP has more of the conformance in its structure. In HL7 in contrast conformance is baked in from the beginning. You have three well-established, well-respected SDOHs, each with different processes. But it results in different types of issues for those trying to correctly implement and utilize the standards once they are adopted.

Our big listening session this past June. We obtained stakeholder to five considerations pertaining to standards adoption and advancement, integration, and measuring the value of standards. After our presentation to the committee in January in which we described the areas of consensus of the Subcommittee, the Subcommittee then took those areas of consensus, put them out for the public to kick the tires, and then in the June listening session, we obtained that insight from the participants. We asked the participants whether the considerations should become recommendations to be sent to HHS, whether the considerations as described were really actionable by HHS or other parties, whether or how the considerations could be used to support action or changes by other relevant organizations like the standards development organization themselves, but also with some particular thinking about the vendors who actually developed and supplied the covered entities with the software and technologies to handle the transactions. And then the required statement, other opportunities, anything else that they would like to comment on.

Here are the five considerations that were specifically addressed in June. As you will see as we get into today's language for the recommendations with the exception of number three, there is not a whole lot of change. The first consideration was to allow adoption and use of more than one standard per business function, meaning you could have different standards or organizations all have an adopted standard that did a particular function like prior authorization or a claim and given the appropriate rulemaking processes to initially adopt those standards, what we are saying then is that CMS could and should as appropriate, allow adoption of multiple standards to achieve the same business function.

The difference in technologies between standards development organization A and standards development organization B could then be best gauged by the particular populations of covered entities that would or could be implementing those standards. Important to understand that this is not rip and replace. We would not repeal – we would not propose to repeal of any of the existing adopted standards and the industry would be certainly well advised to continue to use them where they work well and specifically, we look at the NCPDP transactions and certain of the X12 transactions, specifically, the three claims 837s, health care, institutional, dental, and professional and the payment remittance advice. Those claims and remittance advice have adoption rates within industry of over 90 percent according to CAQH CORE's index. And there is certainly nothing we want to do to adversely affect the installed base.

What we are looking to do is allow others new implementation for those for whom some of the standards just do not work for their business purposes and within their workflows to look to other solutions, possibly APIs, application programming interface. The ones receiving the most conversation right now is HL7's FHIR. As the FHIR implementation guides become available, those would be considered for adoption, irrespective of whether there would be existing adopted implementation guides from one of the other SDOs.

Consideration 2 would be to allow multiple versions to coexist simultaneously. Currently, HIPAA allows one and only one version to be in effect at a time. Each time a new version is adopted by CMS, there is a transition window of a specified duration. At the end of that window, all the covered entities must be completely moved over to the new transaction version and the use of the previous transaction version then becomes prohibited. We are seeking to change that and allow the older version to remain in use by those who get no business advantage, who do not have a business need for the updates that are included in the newer versions. We think there can be some cost savings and burden reduction by allowing industry to have multiple versions in effect at the same time.

The Subcommittee also heard information that in industries other than health care, the support of multiple transactions, multiple versions is very commonplace and that the expertise among large organizations to support this kind of multi-standard, multi-version is routine and is manageable.

Consideration number three. This is the one that addressed the exception process for willing trading partners to test emerging standards and the production mode. The feedback we got from the June 9 conversation with industry is this was not an issue that was on anyone’s critical path. We had a number of commenters who supported the need to revise the exceptions process as it now stands. We had a number of commenters that liked the way the exception process now worked.

In its analysis of the testimony we got on June 9, the Subcommittee decided by consensus to remove consideration number three. You will not see this among today’s recommendations.

Consideration number four was to identify options for improved integration of health information standards, including not just the base standards but the implementation guides, more broadly that at present. And what that essentially means is that the standards have to be put brought into use by more than just the HIPAA-covered entities.

To do that, the thought of the Subcommittee is that there has to be a convener found at the federal level to create a venue that will foster collaboration across not just the HHS agencies and offices you see here listed and some of the other federal agencies as well, but also and importantly to include state, local, tribal, and territorial governments. This, we did get a lot of comments on. As I have mentioned before, we have changed the packaging. But the fundamental essence remains and this has become recommendation number three.

Consideration 5 was to develop a guidance framework that would allow different actors within industry to in a consistent way have definitions, have metrics, have various templates, have pilot test procedures, and reporting standards to actually measure and report on standards, the readiness of standards, on the cost of proposed new standards or updates to existing standards, to convey the results of real-world testing and the metrics essential for the overall evaluation. We think this would better enable measurement, management, and understanding of the standards, and very importantly here, the net value of the standards. Too often, we, the industry, we, as the US system, to keep general results to a very I would say almost an accounting approach of measuring cost. But we do not have a really good way of measuring value.

We can come up with what it might cost to – some really broad-brush ballpark estimates of what it might cost to implement a new standard. But we do not have a really good way of measuring the value of the standard nor do we really include a process where we compare and contrast the cost of implementing a new standard with the cost and value, positive or negative, of staying with the old standard. What we get is because we can establish the cost of a proposed new version, we only look at the cost and say that is expensive. We do not want to do it.

What this recommendation will go to is saying you have to also have to look at the relative value. In the long term, we do not get value from the old standard so that in itself is a cost. How do we measure the proposed new standards, again, value to value rather than just the implementation cost, which we know is a big ticket?

Here is the language for the recommendations that you will see will be going in the letter. We will look at the full letter later on. But for this portion of the agenda today, we are just going to focus on the language of the four recommendations themselves.

What we framed as considerations back in June, we have not gotten the public input. The Subcommittee had an internal discussion and analysis over the couple of months since then. As I mentioned just earlier this week, we had conversations with ONC and CMS.

Based on all that, here is the language for the recommendations for your consideration today. One, update relevant HIPAA policies to allow the adoption and use of more than one standard per business function. As we get into the letter and some of the more detail, you will see some of the explanatory language. But this is the recommendations itself. This is the fundamental, the core language.

Recommendation 2. Enable HIPAA-covered entities to support one or more versions of adopted standards for business functions. For those of you on the committee who are not into the HIPAA weeds, the covered entities specified by HIPAA are three very specific entities and that is payers, provides, and clearinghouses. Those are defined as any of those three that conduct operations, conduct transactions electronically. If you are a payer or a provider or a clearinghouse and you conduct any of the covered transactions electronically, you must use the HIPAA adopted standards.

One and two is the number standards. Two is the number of versions of standards in effect at one time. Recommendation 3 is recognizing the Office of the National Coordinator's existing authority to facilitate the coordination of social determinants of health efforts across HHS agencies and offices. HHS should expand ONC's authority to include a formalized public process for convening non-federal entities, specifically state, local, tribal, territorial governments and to align reporting requirements and federal opportunities. HRSA, SAMHSA and CMS are cited and as Sharon mentioned in her presentation. There are other federal agencies with programs and regulatory authority that complement HIPAA. They kind of need to be brought into the fold.

Recommendation 4. HHS should develop and publish a guidance framework for Standard Development Organizations and other industry stakeholders that outlines how to develop and report quantifiable estimates for new and revised standards readiness, costs, and overall adoption value to support HIPAA standards development, testing, evaluation and adoption. This is a theme that has been identified by the Subcommittee by our hearings over the last years that part of the rulemaking process requires an impact assessment on industry impact assessment and also requires a fiscal impact assessment. To date, that has not been accomplished well in part because the responsibility for developing the standards lies with the SDOs but the responsibility for documenting the impacts and cost fall with the CMS division and national standards under the Federal Administrative Procedure Act. DNS has to do these kinds of studies and come to these kinds of conclusions in order for a rule to be proposed.

And what the Subcommittee is saying that the current system has not been working well. There is just not the kind of data that is produced during the development that supports the DNS' effort to put together its impact analyses. And to the extent that we can push, we, as NCVHS, can promote pushing the gathering of data out to the early level where it is considered by the SDOs during its routine process for considering all recommended updates to the standards that this would serve as useful information of the industry because the industry itself is demanding it. It would serve as useful information to the SDO to help them decide or prioritize the criticality of any one proposed amendment or update to the implementation guide. And then very importantly, it would give the Division of National Standards much of the data that DNS would otherwise have to figure out some other way to gather for it to do its prep work in putting together a notice of proposed rulemaking for the adoption of that standard or that particular implementation guide.

I think I have covered a lot of this in my explanations. I will skim through this fairly quickly. In recommendation number one, this is about the adoption and use of more than one standard per business function. We received a lot of testimony that the newer technologies could be more effective and efficient for certain of the transactions, not for every transaction and certainly not for every covered entity. But for a number of the transactions and for large components of the large sectors of the covered entities, there would be efficiency, burden reduction, improved workflow, and reduced cost if we allow different technologies to address the business needs. As I also mentioned, it is important not to disrupt the installed base. We are not saying rip and replace here.

In case and point, one of the comment leaders we got on our listening session was from the American Dental Association who essentially requested that – suggested that the X12 transactions were not working for the dental industry and that the ADA would prefer either a FHIR-based solution or something similar to that or the needs of the dental industry to be met more efficiently than the existing X12 transactions. That captures the thought of the Subcommittee that allowing a variation like this would be better than the status quo at achieving when measured globally the efficiencies that are one of the objectives of the HIPAA admin simp transactions and standards legislation.

Recommendation 2. Again, supporting more than one version of adopted standards. There are difficulties moving to a new version in lockstep. Everybody has to convert it once. It stresses resources. You have to do the education to your own – any organization has to do the education to its own employees. Then each organization has to test with all its trading partners. If you look at it from a health plan perspective, health plans will have thousands of provider practices to test with. If you look at it from the provider practice, I think Medicare statistics say that each patient – long speech. The statistics show that most providers deal with dozens of different payers. You have a huge version to get all those connections tested individually. All the glitches worked out. And, again, when you are trying to do this, you have multiple health plans dealing with a provider practice. You have a provider practice dealing with multiple health plans. If there are issues to be fixed, if anyone fixes an issue with one provider, there has to be a quality control to ensure that that fix for it to make the one trend connection work will not break the dozens or hundreds of other connections that have already been set up.

By allowing multiple versions on a use case by use case basis, not all trading partners would be required to upgrade. That would significantly reduce the cost of upgrades for entities who do not have any value to be gained in the new version. It would also reduce the number of trading partners who have to go through the end-to-end testing. We see that as a win-win for the industry.

Recommendation 3. Recognizing ONC's existing authority to facilitate the coordination of SDOH efforts across HHS agencies and offices, expand ONC's authority to include a formalized public process for convening non-federal entities, and align reporting requirements in federal opportunities.

The Committee notes and the panelists confirmed that collaboration and coordination on harmonization of data elements, data content, and data exchange exists between a number of federal agencies within HHS including CMS, Office of National Coordinator, Office of Civil Rights, Centers for Disease Control.

Building on that collaboration to attain other objectives for harmonization is complex but has transformative potential. That means there are other entities that could very much benefit from that type of collaboration and coordination that are not included in the existing ONC program. We are suggesting that HHS could build on the momentum by considering establishment of a joint governing entity with authority to support additional work on content structures and formats between diverse data sources, development of standards for missing use cases, implementation, and test tools.

Seamless exchange of SDOH data across public and private settings provides the potential to identify and address health disparities and increase overall population health, and not just limited to SDOH but other types of data exchange that crosses the different agencies both federal and non-federal and the different programs would also benefit by having a structure and a menu at which all these data use needs and data collection needs could be considered and ten coming out of that venue of course would be valuable information for implementers, feedback to the SDOs, information to either ONC or CMS and the regulatory capacity and then information to CMS and the other departments in their Medicare/Medicaid other program administration responsibilities.

States and tribal, territorial, local officials would also then be free to use the nationally adopted template or nationally adopted standard for their local jurisdictions because they have had their input. They know their needs will be met. And that way their state staff will not have to go through the effort of designing and building a one-off standalone unique proprietary system. And then all the providers or payers or others who contribute data to that system have the advantage that there is a single uniform structure that they can use to report to all the different agencies across whatever states, territories, or local regions, including the federal reporting requirements and program reporting requirements. There would be much value to be gained by incorporating the state, local, tribal, and territorial data needs into a more nationally coordinated template, if you will.

Recommendation 4. HHS should develop and publish a guidance framework for standard development organizations and other industry stakeholders to essentially develop and report quantifiable estimates for new and revised standards' readiness, costs, adoption value, testing, evaluation, and adoption.

Some of the standards development organizations are developing projects and metrics to evaluate the standards with both quantitative and qualitative measures. Some standards, such as HL7, undergo a process of testing in controlled environments prior to being implemented to demonstrate their capabilities, functionality, and fitness for purpose.

An evaluation of governance structure or framework could be a partnership between the public and private sector, including appropriate HHS agencies, SDOs, industry stakeholders, supported with regulation or sub-regulatory guidance from HHS. Again, this is taking a page out of the ONC playbook when it is set up a framework on its what is now promoting interoperability and the EHR certification program. We know what we are going to measure. Setting that up, setting the test beds, setting the reporting templates, setting up the – essentially a set of standards for how we measure and report we think would be helpful across the board within the standards adoption world, particularly for HIPAA but not limited to HIPAA.

Next step is we will have a discussion here, as usual. First off, any questions, clarifications, what not. And then we move forward and review the letter. Once we get through the letter discussion, assuming that questions are addressed and any necessary changes are identified, we would – upon approval by the committee, we would send the letter of recommendations to HHS. And then we would continue our engagement with both OBRHI and ONC.

Before we open it to questions, let me pause and ask Denise if she would like to add any comments to what I presented. I know it is a lot. Some of it was down in the weeds and it wandered a bit but there was so much to cover. I am hoping I hit the key nuggets.

Denise Love: Rich, you did a great job. I have very little to add except I just wanted to close with the fact that we are really asking so much more of our administrative data systems than we ever have had to before. This effort is trying to support this transition as we use the data beyond paying claims for value-based care, population health, and public health reporting. These systems are filling a critical role. I think you communicated this.

At this transition, what we are trying to do is to adapt to new technologies and accelerated use cases with as little disruption as possible but moving forward, nonetheless. I think you covered the weeds very well. Thank you.

Rich Landen: With that, let us open it to questions, comments from anyone on the committee. Maybe it was a bit much of a fire hose. There is Melissa. Melissa, please.

Melissa Goldstein: Hi there. I have a very small comment and I wanted to thank you for such a – the fire hose is appreciated. Thank you for such a comprehensive description and explanation of reasoning, which is very helpful to me. I am sure it is very helpful to others as well.

Could you go back to – I think it is Recommendation 2. It might be Recommendation 3 that my comment is. It is about the social determinants of health.

Rich Landen: That would be three.

Melissa Goldstein: Number three. Okay. I am looking at the language of the recommendation itself. I think a little bit more detail might be useful in just the language of the recommendation. Where it says recognizing ONC's existing authority to facilitate the coordination of social determinants of health efforts across HHS agencies and offices, I might specify and however you think the best language is. Are these data exchange efforts? Are these reporting efforts? Are they reporting requirements? That it is not all social determinants of health efforts across the agencies. That we are speaking specifically of standards and data reporting and that world, our NCVHS standards world. I just thought a little bit more descriptive language there might help.

Denise Love: I think we were referring to the content standards, data dictionaries, a centralized place for implementation guides, data dictionaries, a centralized place to go and to update those standards. It is not just exchange.

Melissa Goldstein: But it is also not everything we are doing, everything that the agency is doing about social determinants of health, which is what it reads right now. It is just general authority to facilitate. And ONC does not have necessarily, and Sharon could obviously help us with that. But I think it needs to be more specific than it is right now.

Denise Love: Maybe instead of efforts, are you saying maybe standards or standard development and implementation? Would that be clearer?

Melissa Goldstein: Yes if that is accurate. You guys know much more than I do about what it would be and accurate.

Denise Love: The whole enchilada. I think what we are meaning is the package. What I am hearing is a conceptual framework and centralized place for these definitions and implementations of social determinants of health data elements.

Melissa Goldstein: It has to, I guess, describe what ONC's authority would be as opposed to the other sub-agencies within HHS. For instance, ASPE has a larger purview than simply standards. That is what I was looking for there was some descriptive --

Denise Love: -- is the problem. We will have to clean that up, I think.

Melissa Goldstein: It is not a big deal. It was just a question that came to my mind.

Rich Landen: One of the things we are dancing around here is that when NCVHS makes recommendations to the Secretary, the guidance that the Subcommittee has been given is we are not supposed to specify which office within HHS the Secretary should assign. What we are trying to do here is recognize that the recommendation really goes to an existing charge already in effect on ONC and we are essentially recommending the expansion of that charge, not the delegation, not specifying delegation of something to some agency within HHS. But your points are well taken and we will take that back and work with staff to try and address the specificity there. Thanks, Melissa.

Valerie Watzlaf: Thank you. Thank you, Rich. This is excellent what you have done. I am also still learning so much about this. My question, I think, was in Recommendation 4 because I was, I guess, kind of also wondering – I believe you were saying it is a way to measure the value of the standard. And I think also you brought up some interoperability there. But I was just wondering. Who would actually do this? I know you talked about the SDOs, but then would it be I guess working with what other groups if there could be more specificity there. I was not sure if you were able to do that though.

Rich Landen: Yes. Thank you. Again, as I said, our instructions, if you will, are not to name the agency. But it is our understanding and our assumption that this would fall within the scope of OBRHI, the Office of Burden Reduction and Health Informatics. As I mentioned a couple of times, we had a discussion with Dr. Mary Green, in whom you have met at previous presentations to the committee.

Among the offices within OBRHI or the departments within OBRHI is the – Lorraine, correct me if I misspeak. The name changes and I am an old guy. I cannot keep them straight. Division of National Standards. DNS actually is the one charged with doing the kind of impact and fiscal analyses that I referred to. Our assumption is we are working with OBRHI on this.

We do have ongoing – we, the Subcommittee, do have ongoing conversations with OBRHI, as we do with ONC, and have discussed this with them and are intent about what this would mean. It is to essentially – I like to use the term that I picked up from an aviation standards group presentation to health care that talks about the checklists that the pilots use before takeoff and even experienced pilots. If they do not have a checklist that the industry refers to as "plastic brains". Everyone once in a while they forget something on the checklist and that has some bad consequences.

As some of you may or may not know, that concept was brought into health care many years ago specifically for surgical procedures. There are checklists, sponge counts, you name it. We are taking that concept here. If we had this kind of a checklist that has what are the data bits and pieces that we need for various purposes and we look at that as early in the standard development process as we can. That is what we are trying to achieve here. Not only would the SDOs use it to help prioritize their standards and help package them as to here is the change we made. We know it is going to cost a lot of money but here is what you get for that.

Again, you have implementing organizations, trade associations, trying to understand here is this standards version update. What is the value to us? Why are we better off with it than without it? And then finally, HHS itself, Division of National Standards, in order to populate the data, the evidence, if you will, in the impact analyses, they would have the majority of this data rather than having to take the time and go through the expense and hassle and trying to locate authoritative sources of this data. Most of this data then would come along with the newly-proposed standard from the SDO and would eliminate an awful lot of delay, an awful lot of duplicative work and most importantly, eliminate the – not eliminate but it would do the education by which industry could make its decision on is this valuable to us relative to staying with the previous version.

Valerie Watzlaf: That is great. Excellent. It is kind of like the patient safety quality improvement checklist that we have used before too. Thank you. That really helps. Thanks so much. Great job.

Rich Landen: I do not see any other hands. Let me invite the Standards Subcommittee members to chime in. This is your work. You have done a ton of it and a lot of good deliberations. Here is a moment for you to shine if you choose. They are all so modest.

Denise Love: I wanted to acknowledge the Subcommittee. We have worked I think in the last year harder than all the years that I have been on this committee. The knowledge base is tremendous. This reflects hours and hours of deliberations by the Subcommittee and input from the industry and Rich's expertise. I just wanted to give a shout out to everybody.

Rich Landen: You will hear this afternoon that because we have done such good work, our plate is even fuller going into the next quarter and fiscal year but more of that later.

Vickie, your hand is up.

Vickie Mays: Can you go to Recommendation 3 on social determinants of health? I apologize that I did not see this before. I am trying to think of – it is very small but I want to make sure it is okay because – where it says the seamless exchange of SDOH data across public and private settings provides the opportunity to identify and address health disparities and increase overall population health. The disparities are merely differences, and some differences should be there. But I do not think this needs to be in equity. I was trying to think of how to modify it because some people would say a difference is a difference. But you still want them to go to the next step of if that difference should not be a difference to make sure that they are going to address it.

I am supportive of SDOH being there because of the timeliness. Every different place that I think we can get this in we should. It is in the workgroup charter, but I think it is going to be a bit of time before we can get to it.

The question is I know what you mean. I do not know how to fix it a little bit.

Denise Love: The third bullet, Vickie? I am trying to figure out what the fix is and what the issue is.

Vickie Mays: The fix is just health disparities. In health care, we know that there may be different values, different outcomes, and they are not necessarily bad. I remember we did this in Healthy People when I was on the National Academy. We were making sure. It is almost like we started using the term better than the best to make sure that it is just a difference. Some people sometimes do not fix. I will leave it. And if I can think of a modifier, a different word, I will give it to you. But I just want to hold people a little bit more accountable that they do not say differences are acceptable but that they go further to investigate whether that is a difference that is not acceptable that should be addressed. I will have to think more about it. It is fine. I am being really picky. I have been in enough settings where sometimes people come up and say these things. Just because it is a difference does not mean that we have to jump at doing something.

Denise Love: I think maybe instead of identifying is to measure because at the local level, they are not able to really measure at a subpopulation level in some cases to discern Asian populations, for instance. We heard this. We heard this over and over. I think what we are trying to do is get at the granularity so that they can measure and address it. But right now, I heard, and I can testify it is not getting there.

Vickie Mays: You just came up with what I think is helpful. An increased overall subpopulations health. That is it. It is not about just the population as whole, but where we are trying to focus is on a more granular level of subpopulations. To me, that would be the great fix. I am happy if you will accept that.

Denise Love: I would like to hear what Wu Xu says too, because she is expert in this.

Wu Xu: I was thinking if we change disparities to bring equality, address health equality and increase whatever Vickie suggested, the subpopulation. I think if you just say subpopulation, it is too general. Maybe disadvantaged population.

Denise Love: Vulnerable or at risk. I think those wordings are easily done. We have massaged this – that the overall buy-in was I think presented to the committee and then the listening session validated this. But it has been really a lot of work to make sure we acknowledge the current work going on through ONC and the department because there is a lot of work going on.

And then what we are trying to do here is just expand that work to this local – state and local and also other government agencies with administrative data sets, as Rich said, but also, a go-to place for state and locals and guidance tools, all of that. I think we can word this very easily, Vickie.

Rich Landen: From the process standpoint then, Denise, are you assuming ownership of Vickie and Wu's comments when we start looking to see how we tweak the letter. I am not sure if Lorraine is on the call with us or not because I think she would be critical to address Melissa's comment. For process, we need to figure out what we need to change when we get to our next step, which is review of the actual letter itself.

Denise Love: And I also forgot to say that the staff, Lorraine and Rebecca and others, have hung in there through this whole process and kept us moving forward. Again, a great thank you. It has not been a trivial undertaking.

Rich Landen: -- been without pain but hopefully, pain is gain.

All right. If we can move then to the PowerPoint to the letter itself. Most of the – the first couple of paragraphs are pretty much our standard boilerplate letters, obviously, addressed to Secretary Becerra. The first paragraph says who we are and why we have standing on this matter.

The second paragraph talks about some previous work and then we get into the change of the environment, recognize new drivers of transformation and health care data exchange. Let us just take a minute – anybody, any committee members with comments on the first two paragraphs.

Hearing none, can we scroll down?

Rebecca Hines: You failed the spellcheck test, guys. It is NCVHS.

Rich Landen: I have yet to do my final review for whether HIPAA has one P and two A's or two P's and one A.

Maya Bernstein: We got that right. We would fire you immediately. Everyone here knows the answer to that.

Denise Love: This is the version you saw this morning that we sent around.

Rich Landen: The next paragraph we talk about why this is within HHS' purview. We talk about interoperability, data sharing, information blocking, the convergence that we have been engaged with, HITAC, ICAD. In this letter, we are submitting four actionable recommendations for consideration to bring data flows in HIPAA transaction standards into optimal configuration to regain the efficiencies and visions in the original HIPAA legislation. Further details appended. We tried not terribly successfully, but we tried our best to minimize the verbiage in the letter itself and do a lot of the explanatory materials in the appendix. It has grown. The letter itself has grown but I do not think it is outside our norms or parameters. But this line does refer to the appendix.

Recommendation number one, which is what we discussed about allow adoption and use of more than one standard per business function. Specifically task an HHS office to collaborate with NCVHS to develop a systematic approach to evaluate, plan, and if proven, implement multiple standards for HIPAA.

Bullet two. An example of the usefulness of a multiple standards approach is the emergence of new standards to support electronic prior authorization. A second example is pointed out in the ADA public comment letter that would allow small practices to use relatively less complex standards like FHIR while large organizations would be free to use the more complex standards like X12.

Bullet three. HHS --

Vickie Mays: Again, this is just a very small thing, but I do not know. For reason, it is bothering me. You have update relevant HIPAA policies. Isn't update-specific HIPAA policies? Don't you have very specific things that you want them to do? Are there other things – relevant? It kind of leaves the decision making up to them. I do not know. Maybe we are supposed to do that with the Secretary. But don't you have very specific things you want them to do?

Rich Landen: As always, your questions force a lot of thought and are much appreciated. Relevant was chosen consciously and I think our discussion is because we, on the Subcommittee, are not always aware of exactly what these policies are in existence and what – in this specific instance, the Division of National Standards has to comply with either publicly known policies or internal operating policies. You are absolutely correct, Vickie. We want some specific fixes or specific changes. We have that specificity, but we are not sure about which policies will be impacted by our recommendation. That is why we chose relevant.

Vickie Mays: I can see that actually is greater accountable and then I am fine with that because it says this is what we know. Here are the specifics. But you are also holding them accountable for things that internally they may know and should be also included. They are relevant actually. I applaud you because I think that that is a smarter word to use.

Rich Landen: And, again, for the general edification here that once CMS or any federal agency goes into a rulemaking process, they are prohibited by law from discussing that externally. Externally would include us. There is a lot that goes on in the rulemaking process that we are not and never will be privy to.

Denise Love: There may be policies that are not rules but that we have no way of knowing internally what they are.

Rich Landen: Any other questions on Recommendation 1?

Recommendation 2. Support multiple versions of adopted standards. Specifically task an HHS office, again, we are assuming OBRHI, to collaborate with NCVHS to develop a systematic approach to evaluate, plan, and if proven, implement multiple versions for HIPAA. An example of the usefulness of the approach is the device identifier, specialty practices like cardiology, routinely implant pacemakers and would have a business imperative to implement a new version that carries device identifier data. Just as an aside, the current adopted transaction standard for the X12 837 claim does not have a data field that would carry a device identifier. The newer versions that will be proposed do have that incorporated into the base standard, into the implementation guide.

Back to the bullet, in contrast to a practice like cardiology, a dermatologist may never implant a device and would not need that upgrade. That means the multiple versions policy would say that cardiology practices would update to the newer version of the X12 837 claim standard when that is adopted as a final rule by CMS. But the dermatology practice would not have to move to the newer version of course unless there were other things in that version that were applicable to dermatology. The current situation is that everybody irrespective of business need must update. And what we are proposing here is the updates are discretionary based on the functionalities enabled or supported by the newer version of the standard vis-a-vie the current version of the standard.

Installed bases protected. By installed base, we mean everything that everybody has implemented, the hardware and software that they are running on now. They would not have to be ripped out and replaced just for the sake of meeting a regulatory requirement.

Fourth bullet. HHS should ensure that regulations allow multiple versions of standards, i.e., one, two, or three versions of implementation guides or implementation specifications to coexist as they are tested and used by stakeholders to meet specific business needs in addressing gaps while preserving ongoing use of widely used existing versions.

We point to the Office of the National Coordinator's Standards Version Advancement Process, SVAP, as a success story and a potential model. The way things in ONC are done with promoting interoperability program and the certification program for electronic health records uses a different model than DNA uses for the HIPAA transactions. We are suggesting there maybe synergies, if you will, if CMS would look at SVAP and could possibly do some adaptation of the HIPAA processes.

We encourage HHS to continue working with the SDOs to ensure compatibility between versions of standards and to enable the use of new versions through the regulatory process. The point here is in the industry, the term is backwards compatibility. If a new standard comes into being, there should be a way to map from the old standard to the new standard. That is an ongoing challenge. But the SDOs are getting better at that over time.

The other thought that is embedded here without explicitly being stated is that the data definitions, the data fields, the data structure is all compatible across versions.

Questions on Recommendation 2? I see no hands. Fair warning. Move to three.

Recognizing ONC's existing authority to facilitate the coordination of SDOH data standards efforts – thank you for the modification, Rebecca – across HHS agencies and offices, CMS, ONC, CDC, NIH, IHS. HHS should expand ONC's authority to include a formalized public process for convening non-federal entities (e.g., state, local, tribal, and territorial governments known as STLS) and to align reporting requirements in federal funding opportunities, e.g., HRSA, SAMHSA, CMS.

Rebecca Hines: Rich, Vickie's hand is up.

Vickie Mays: I am trying to understand why it is requirements in federal funding opportunities.

Denise Love: The harmonized reporting templates requirements across different grants that come out from the federal government to the locals so that there is some harmonization in the reporting requirements.

Vickie Mays: I am not sure that it should be in the funding opportunities as much as just in the federal reporting opportunities. The reason I say that is in a grant, you are going to study these things sometimes. If you do this, the ability – this is like what is happening at NIH that people are getting upset about. You are being told to use RADx and something X and all these things. I do not think it is about the funding opportunity where you are told before you even start. It is about collecting that data in that funding opportunity in a way in which when you report.

We have a form that says report on who participated and all this other stuff. You want that in the form but not the requirement of the way in which to do the reporting. All you have to do is have the form in there. I want to make sure they do not interpret this the wrong way.

Denise Love: Program reporting.

Vickie Mays: It is about a line required reporting that I am okay with. And it should not be just a funding opportunity. It should be in general. We are trying to harmonize what we send from local and states up to the federal government. How we gather it should be up to us. But how we give it should be in that expanded version. If you tell me I have to report my data in a certain way and it does not interfere with what I want to collect, I am happy. I think it is fine --

Denise Love: -- and federal programs --

Rich Landen: I am hearing it a little bit differently and not my area of expertise. But I am thinking back. Funding opportunities to me is not just grants but it is also – not just research grants but it is grants for things like updating a system in which case I would stick with our original thing that the funding opportunity would say update your system. But if you can update your system, your new system must encompass – must support these standards.

Denise Love: This is sort – the data modernization grants being – right now.

Rich Landen: Vickie, in terms of your – specifically, your comment of tell me how to report it but not how to gather it. For some of the discussion topic that we had was the California county by county different reporting instructions for COVID incidents and COVID resource availability reporting, it did seem to the Subcommittee that getting more into the acquisition since the acquisition comes from essentially what we were focusing on in that conversation was acquisition of that information from hospital systems and hospitals then were faced with getting different reporting requirements from all the different counties in California. I would suggest that we add federal programs, but we keep funding opportunities and we connect them by an "or". Would that --

Vickie Mays: What that means is that you focused in on something that has very broad set of differences and investigator initiated then is caught up in this. I understand exactly what you are trying to do. And to align required reporting requirements, system – I think you should have a series of things that you call out because funding opportunities is just way too narrow in some ways even though it includes lots of different things. For some people when they read that, they do not think of other things. If I do not get money to do something, then I do not have to do this. If I get new monies, then I have to do this. That is kind of how it can be interpreted.

I think it is required reporting – too many requirements. Required reporting requirements in federal programs, data system alignments. I think you need to be specific as to the coverage. But it should not be just about a funding opportunity because those are very limited.

Denise Love: I agree.

Rich Landen: Denise, your language before about the system modernization. Would that fit in there?

Denise Love: Yes. One example right now is the infrastructure grants where they are calling for modernization of public health infrastructure and systems. It is very broad, but we want them all to start looking the same way and harmonizing. Align reporting requirements in federal programs.

Vickie Mays: -- systems, in general. Health and health care systems.

Rich Landen: Or possibly, we could use the format we used in the other recommendations and put that detail – that specific program reference in a bullet.

Vickie Mays: Rebecca, it should be health and health care because health care would just be hospitals and what have you. Health would include surveillance. You want data alignment systems. Data alignment, health, and health care systems. I do not want to do this here. I think we have the idea, and we should let you figure out the wording here. It is something like that because I think funding opportunities is just really too narrow. You have my gist, so I am not going to try and wordsmith it.

Wu Xu: I agree. Change federal programs, not use funding opportunities. I worry for the health care systems there because here, we are talking government relationships, federal with the state and territory. The health care system will not require state to do anything. We require them to do our reporting for us. I was just thinking the political system requirement, should we put health care system there? That is my comment.

Vickie Mays: Can I just pose the question of in COVID, we just have this problem of getting, for example, hospital data reported with race, ethnicity, that kind of stuff. That was why I was thinking of health care systems. But maybe it is too comprehensive.

Wu Xu: Actually we can move health care system above before the federal programs. It is the same parallel with the state. HHS convening non-federal agencies and major health care systems to align required reporting. Move the health care system before --

Denise Love: Like e.g., health care systems, state, local, because we are non-federal entities.

Rebecca Hines: Vickie, what do we do with your health? Is it in federal and other health programs?

Vickie Mays: Align reporting requirements in federal. It should be programs, data – I think you need to say something about data systems or data system alignment or something.

I think if we move health care up, it might be okay because ONC actually goes across more than just deals with HHS. Then I think maybe not putting health there but health is implied as one of them. This gets to the multi-sectoral needs that health care data actually needs. If they will do it across other things that would be great. Rebecca, I think I am okay with leaving health out. I have to think a little bit. We can move on.

Rich Landen: See no other hands. Can we scroll down and take a look at the close of the letter then?

Rebecca Hines: This is the old one. It is missing the fours. For HHS. Lorraine, can you remind me of the fours that got dropped somehow? Maybe Rich, if you could go look at the slide.

Jacki Monson: While we are looking at four, is there a reason why we do not have anything under Recommendation 3? It looks weird that we do not have anymore further details other than the recommendations standing alone versus everywhere else. We actually have an exposition of what is included.

Rebecca Hines: Rich, the bullet points did not get brought over this morning.

Denise Love: I can pull those -- I think there were three or four bullet points.

Rich Landen: My apologies then. I missed them in the multitude of versionings going back and forth.

Denise Love: Do you want me to scour those?

Rebecca Hines: Do you have that available so I can stop sharing and you can share those, Denise?

Denise Love: Well, I do not have it up. I do not have the version up. I have other versions and I am worried which version I have.

Rebecca Hines: We do have time on the agenda to revisit this. How about we clean this up and get those added, send it back out, and make sure we can look at those before we vote today or tomorrow?

Jacki Monson: I think that would be good. I think giving the committee a little more time since we just got it early this morning to have the ability to digest it. I would like to push the vote to at least tomorrow to give people the opportunity to review it in further detail. Scrolling through, I cannot read as fast as we are scrolling. No concerns that I have not already raised. But I think we need to give people more opportunity to have the ability to review it in greater detail and provide comments. I would suggest that we move to the vote to tomorrow.

Rich Landen: That would be good. What I would like to do if it is okay with you, Jackie, is just get a confirmation that nobody has any outstanding issues they have already identified today. I looked at the two previous versions of this and I did not see bullets on there. We will have to dig a little bit deeper to find them. But the point is well made.

Jacki Monson: And that works for me, Rich. Thank you.

Rich Landen: Shall we continue to scroll down and see if there are any questions on the appendices then?

Rebecca Hines: Rich, I do not think we did number four, Recommendation 4. Denise or Rich, if you could open up the slides, we are missing some FORs.

Rich Landen: I am not sure which version we have here in the slides.

Rebecca Hines: I can pull it up.

Rich Landen: The versions I have at my fingertip do not include that latest modification. If you have it, that is fine. Otherwise, I will go back to email.

Rebecca Hines: There it is. That is what was on the slide.

Rich Landen: Thank you. Rebecca. Health and human services should develop and publish a guidance framework for standard development organizations, other industry stakeholders that outlines how to develop and report quantifiable estimates for new and revised standards' readiness, costs, and overall adoption value to support HIPAA standards development, testing, evaluation, and adoption.

The framework should include agreed upon definitions, metrics, templates, test methods and procedures, publications of results. It should include templates for – that is duplicative. That second bullet is duplicative. We will need to go back and polish this here.

It should include methods estimating standards readiness, standards cost and overall value, resulting from adoption – should differentiate among base standards, for example, the X12 version 8020 or health level 7, CCDA, implementation guides (i.e., specific use cases utilizing only designated subsets of a base standard). Conformance requirements and operating rules. Is that the last bullet or is there one on the next page?

Rebecca Hines: That is it.

Denise Love: Rebecca, I put the bullets in chat from the last version I have on Recommendation 3 under recommendation bullets. I put it in chat.

Rebecca Hines: The chat is copying and pasting today, I believe.

Denise Love: Basically, it affirms that we heard from panelists in the listening session. We want to build on the collaboration that exists and the momentum that is – to work on the data context structures and formats between diverse data sources and development of new standards – and test tools. And then continue ONC's leadership with this broader or larger collaboration to accelerate and improve the integration of SDOH data at all levels, providing technical assistance and tools. One of these is an example that came up as a virtual EHR for testing purposes and other activities to accelerate and improve integration of SDOH data. These are, I think, the latest version of the missing bullets.

Rich Landen: If there are no questions on these three bullets, we will take another quick look at four. Any questions here on four?

Tammy Banks: We also had a bullet in the previous version about coordinating with the industry. Is that a bullet that we should put back in or are we trying to be more concise?

Rich Landen: Is this under three or four or where?

Tammy Banks: Four. I am sorry. I am still on four. Sorry.

Rich Landen: Four is good.

Rebecca Hines: Tammy, can you say what the topic was? Is it a check for a bullet on --

Tammy Banks: It was organizational input from the industry. I will get the bullet and drop it in chat. I was searching for it at the moment but I could not find it quick enough.

Rich Landen: Good pick up. Thanks, Tammy.

Debra Strickland: I think we wanted to remove the second bullet, right, because it was duplicative of the first.

Rebecca Hines: Denise, I do not know that this was the most current set.

Denise Love: I went back into my email. The one I sent you the other day is the most current for three when we did that scramble.

Rebecca Hines: And then there is a comment on the framing of these that we have been avoiding HHS should -but we do want these to stand alone so we could just repeat the word recommendation. NCVHS recommends that HHS – so each recommendation would be repetitive in that sense.

Rich Landen: That would be fine. Each of the four would start off with NCVHS recommends that HHS --

Jacki Monson: I just want to do a time check. We passed the break time that we should break for. Should we – Rebecca can clean this up a bit and we can come back to it after the break.

Rebecca Hines: After the break, we have an update. I am wondering, Jacki. We do have time tomorrow on the agenda to get back into these if you want to or did you want to do it this afternoon.

Jacki Monson: Rich and Denise, I defer to you. My thought is we got through at least initial comments on this so that we have the ability to look at it overnight and if we want to seek approval tomorrow, which I am expecting we do. Then it probably makes more sense to maybe push – standard topics to tomorrow if needed in order to get through this today.

Rich Landen: I would agree with that but I would ask any of the committee members. What we have not reviewed in the letter so far is we could go into some background discussion that supports each of the four recommendations and then there is an appendix with even more distant data. Unless a committee member wants us to go through the discussion information on the next couple of pages after our break, you can look at that tonight and then we can address any issues tomorrow because I think clearly the substance of the recommendations themselves and the substantive bullets we have gone through. I would not see a whole lot of time-consuming discussion on any of these things in the rest of the letter or any of the appendix.

Jacki Monson: From my perspective, I just think it will be important to make sure we have gone through the whole letter at least once, given that some of the committee members are seeing it for the first time today.

Rich Landen: Question from Tammy?

Tammy Banks: I was just going to add – I sent you the whole bullet lists from before and I think the periodic review may be an important bullet to keep as well for consideration.

Rebecca Hines: Jacki, are you suggesting that we bring this back up starting a discussion after the break?

Jacki Monson: Correct – letter and then cover what we can with the rest of the standards updates.

Rebecca Hines: There is time this afternoon. I do not know how long that discussion is going to go for the other update or did you want to – we just need to update. We can talk offline if you want. We just need to get the agenda for the public who may be interested in an update at 1:30 to know when that update is going to happen.

Jacki Monson: Rich, what is your estimated time that it will take to go through the rest of it?

Rich Landen: I would estimate between 15 to 20 minutes, assuming no substantive discussion.

Jacki Monson: And the other updates that you are providing. Could we consolidate it, if needed?

Rich Landen: I can do an abbreviated report on the Standards, and I think a more important thing is the update from Margaret Skurka on the ICD-11 status.

Rebecca Hines: And also letting the public know the plans for the X12 and CAQH CORE. That definitely needs to happen.

Rich Landen: Happen but I can condense that.

Jacki Monson: Let us do that as a plan for now, Rebecca, is try to fit in whatever we can. We can use the existing time after 4 o'clock, or if the Cyber Panel finishes early, if needed.

Rebecca Hines: Great. We will bring the letter up after lunch then and then whatever time we have at the end of the day, we will return to this.

Jacki Monson: Yes.

Rich Landen: Thank you, everybody.

Rebecca Hines: We are on a break and we are going to resume at 1:30. You are welcome to leave your connection to the meeting on.

(Break)

Jacki Monson: Okay. Let us go ahead and get started then with our afternoon although it is still morning in California so it feels a little weird to use that term, right Vickie? Rich, Denise, turn it back over to you to review the letter and go through the standards update.

Subcommittee on Standards Updates

Rich Landen: I think what we want to do first is just do a quick pass over the rest of the contents of the letter, acknowledge upfront that we have has some discussion over the lunch break. We have a second set of bullets that it seems is a little bit confusing to the reader. The first set of bullets, the ones that appeared, we went over already. They were tightly integrated with the recommendation itself. This set of bullets was from a previous version, and they are still valid but they are – and they are a little broader. They tend to go more into the explanation of the environment into which the recommendations fit. But there are some redundancies and in a couple of little conflicts that we, on the Subcommittee, will take care of tonight. We will do a review and a reformatting.

What I want to do in the next few minutes is just to go over the content that is in here and highlight it in case there are any questions. Again, we are assuming that two things are going to happen. One is all the committee members will have a chance to relook at the letter in anticipation and in preparation for voting to approve or amend tomorrow in the meeting.

And the second is to give an opportunity to any questions and comments on the content of the rest of the letter here. Not to fix things but to identify areas that the Subcommittee members can work on tonight.

Rebecca Hines: Rich, I do think because people would like some time to read the letter if the letter could go out this evening that would be great.

Rich Landen: Absolutely. Apologies for not having this out earlier and in a better structured format. But as I mentioned, our meetings with ONC and CMS this week have precipitated a lot of last-minute revisions and obviously we did well but not perfect. Apologies to the Committee.

Background and context for Recommendation Number One. Again, Recommendation Number One is a change in the existing HIPAA policy to move from one and only one standard per visit function or one implementation guide at the time to more than one.

When HIPAA was signed into law in 1996, this was the first time that standards on a national level had been implemented in health care. Given the constraints of the technology and the general lack of experience and established relationships around standards at the time, the consensus of industry and this is reflected not only in the HIPAA legislation itself but in the two WEDI reports from 1993 and 1994 I think it is that essentially formed a kernel around which Congress developed the HIPAA admin simp legislation. This was the state of the art and the state of the politics at the time. It was a C change. It was very innovative and it accomplished a lot. But it was the first time we have done it. And 25 years later, there are lessons that we can learn and apply.

By now, by 2022, technologies have evolved significantly. Covered entities have much more experience dealing with standards and each other around development and implementation. And the regulation carefully selected – regulation providing the additional flexibility to industry now appears viable as it was not in the 1996. And that viability goes toward achieving the effectiveness and efficiency that were in the original HIPAA legislation and set of recommendations eventually promulgated by CMS pursuant to legislation.

Some of the standards, as I mentioned before, the X12 837 claims, are in use by over 90 percent of the industry, which demonstrates significant value. On the other hand, some standards like the X12 278 referral certification authorization implementation guide have very low rates of adoption by industry, indicating that there are some problems with that. And hence, the two statements that I gave previously – we want to protect the installed base, the status quo. We do not want to do anything to adversely impact the success rate of the 837s. But we do want to take steps to provide the industry with what they need, the transactions they need for which the adopted 278 is not working well.

Public testimony in our review suggests that new technologies, APIs like FHIR, could be more effective and efficient for certain of the transactions. As I said, this recommendation protects the installed base and is non-disruptive to the best of our ability to gauge and given the comments of the public testimony.

We already mentioned the ADA letter so I will not go into that. We can scroll down please.

Recommendation 2. These are the multiple versions. Similarly, as I mentioned before, updates and adoption of some standards are not meeting business needs. Some relatively simple and straightforward updates just are not happening. They are much needed. But because of the cumbersomeness of the process of promulgating updates and new regulations, those new regulations or updates have not been delivered to the industry even though there is industry support, even though they have been through the NCVHS hearing process and we have made recommendations to HHS that they be adopted.

We, the Subcommittee, is seeing an advantage that allowing multiple versions of the adopted standards could reduce the implementation costs and burdens for updates over time and we are looking for Full Committee concurrence with that of course as part of the recommendation discussion.

There are practical difficulties for moving the new versions in lockstep or demonstrating industry-wide value. Updated fields are only required for some sub-segments of the industry. A pragmatic challenge of end-to-end testing with all the trading partners. I talked about that a little bit more this morning. Allowing multiple versions. Not all trading partners would be required to update. Eliminating cost and effort for many in the industry.

The role of contemporary interoperability is built upon a model in which things move incrementally. The standards should be developed in an agile fashion. That is a term of our agile fashion. So that innovation would be robustly encouraged, and backwards compatibility could be assured.

Agility and agile development go to quick responses, small changes that go to proof of concepts and then testing. If a proposed upgrade or proposed new version does not meet specifications, it is discovered early in the testing. It is not put through the rule promulgation process and industry moves on then to a new attempt to develop an updated version that meets the needs. Again, agile is the key word there.

Recommendation 3. ONC's role in coordinating social determinants of health and in other information both within and outside the federal government. We have talked about that.

The Subcommittee notes and we had discussion at the June 9 listening session that collaboration and coordination of data elements, data content, data exchange exists between a number of the federal agencies. However, the data flows from providers to payers and other non-federal authorities in the existing interagency collaboration. I think that is inter rather than intra. Sorry about that – is not adequate to ensure that all uses specifically both federal and non-federal are incorporated into a national collaboration, meaning that the state, territorial, tribal, and local governments do not get their needs – do not necessarily get their needs met in a national collaboration.

Building on expanded collaboration will be complex but we think it will be transformative. We can use existing HHS momentum to build on and considering a joint entity with authorities, support work on content structure and formats between diverse data sources. This goes to some of the conversation where it is the SDOs. It is the state and local government. It is those in the organizations, institutions that provide the data. It is in the exchanges that make sure the data get from where it is captured to the point that it needs to be reported. Develop new standards for use cases for which there is a need then identify that those use cases have not been developed and for uses in implementation and test tools.

We are looking for national leadership to establish a series of actions and tools to achieve the objectives of a cohesive process and common basis standards across federal industry, state, local, tribal users, and importantly, to provide educational resources for stakeholder engagement.

Testimony to the Subcommittee. It was pretty clear that state and local authorities would welcome a national collaboration to meet their needs. I guess two things to point out is one, we are not talking about a federal mandate. We get into state right issues. No way do we want to go with the federal mandate. We want the feds to put it together. Here is the template. Here are the "standards." That means that the local authorities would not have to invest the money or the resources in developing their own standard and then those organizations and entities reporting to the local authorities would in essence have either the same or a similar reporting demand from the various authorities that they need to report to.

I see a couple of hands up. I think what I would like to do is finish the report recommendation and then we will open it up for questions. Scroll down please.

Fourth is developing the guidance framework by HHS. Again, the language here needs to be tweaked to be identical with what we did and what we read previously. But the bullets. The committee received input about the need to evaluate the value of test updated new emerging standards before they are adopted under HIPAA. Ensure that they function as in intended and meet identified business needs.

For members of the Committee and even the Subcommittee, who are not into the weeds with the standards development and adoption, HIPAA did not include any testing requirements. HIPAA requires only that the SDO approve through its internal process, which needs to be ANSI certified, must develop and vote on and adopt the standards and then bring them through the designated standards maintenance organization to NCVHS for a recommendation from NCVHS to the Secretary of HHS before HHS, meaning CMS and the Division of National Standards, would decide whether or not to begin the rule promulgation process and the adoption timeline.

The problem with that is there is no testing requirement. If something begins, passes through and gets into the regulatory development, CMS publishes a notice of proposed rulemaking, which requires public comment. If things come up in the public comment, there is really no way to go back and fix the proposed rule from the standards organization without essentially redeveloping and – validating that issue, which is a multi-year process. If you cannot go back or if you have to go back and do a two-year process and then you bring it through the whole process again, that is just not a recipe for success if any. It creates a system where it is pretty impossible to fix defects.

What we are talking here is let us do all the testing. Let us agree upon what testing needs to encompass, how to do it, and let us do that before we get to NCVHS and before we get to the rule promulgation process initiation by CMS.

Some SDOs are developing projects and metrics to evaluate their standards both quantitatively and qualitatively. Some standards such as HL7 FHIR, both the standards and implementation guides, the use cases undergo a process of testing in controlled environments prior to being voted upon and implemented to demonstrate capabilities – for purpose. An evaluation of the government structure and framework could be between – could be a partnership between public and private sector, including HHS, SDOs, industry stakeholders, trade associations, professional societies, supported with either regulation or sub-regulatory guidance from HHS.

And then finally, any such structure that gets established should be periodically reviewed to ensure that it continues to maintain its currency, maintain its value, maintain its role in the standards development and rule promulgation process.

Questions? Vickie, please.

Vickie Mays: Can we go to three? Rich, I am very happy that we found these bullets because it really helps me to understand a lot better what you were covering so that is helpful.

But I want to say what you said actually makes this clearer than what is written. When we go to bullet three, this entity could provide national leadership. What you talked about in terms of specifics of developing use cases, providing materials to states, which is what I think you want to put in there. I do not know if you can get the transcript fast enough but that was actually a lot clearer and I think important because it really says what you want them to do. This is kind of like a very high-level do something. But I think it would be better if you said a little bit better what they can do. I think the use cases would be great. I learned from Jamie how important use cases are, for example, in helping people to move along. If you could capture what you said and put in there, I think it would be great.

Rich Landen: I think that is helpful. Thanks, Vickie.

Denise.

Denise Love: The recommendation is not what we revised this morning.

Rebecca Hines: That is right. I think the second half of the letter Rich did not get to before he sent it out. That all has to be updated later today. This whole thing needs a scour.

Rich Landen: I think that reaches the end of the letter. The only thing else on the letter is the signature. After that, we go into the appendix. This provides a little bit further background. I do not think there is anything in here that we have not in some way or another referenced or explained in our presentation today. Again, the go forward plan is for the Subcommittee and staff to work on making the fixes that we have noted as we have gone through the discussions and the questions and comments and observations. We will do that as soon as we can after the meeting today. We will send out a fresh version to the committee members to look at tonight and then we will bring this back tomorrow for some final discussion and hopefully we will have fixed enough that we can bring it forward for a vote to go forward as a letter of recommendation.

Any other questions or comments?

I think then we are ready move into the --

Vickie Mays: Two things. We are going to have a panel tomorrow with the tribal groups. I would suggest that you also see if there is anything in this area that might be useful to them that would help you flesh it out. That is one thing.

The second. Rebecca, I just do not know how we do this. But there was a comment from Alix in the questions and answers that – question-and-answer section about substituting the word data systems. I do not know if we should do this now while we are --

Rebecca Hines: If we were meeting in person, members of audience would not speak up. It is the members' prerogative to review things that get put in the chat and it is the members' prerogative to follow up this evening or not. I think some of the things are helpful.

If you would like to take up someone's question and bring it to the committee now, that is another story and you are welcome to do that.

Vickie Mays: I would like to bring up something I saw in the questions and answers, which is using the word data systems and inserting that. I just do not want us to lose that because I think it was part of what we were struggling to do. We do not have the revised one.

I will just say to Denise and Rich to consider using the word data systems in terms of the health care is to consider either adding data systems or replacing it. To me, it would be both. I did not want us to lose Alix's comments because I thought it was useful.

Rich Landen: Specifically, Vickie, you are saying in Recommendation 3 in the parens that now reads, e.g. health care systems. We would change that to e.g. health data systems.

Vickie Mays: I think you need to just take a moment when you are doing the revisions to see whether you want both/and. I think it is like adding it as additional – that was her suggestion. I am just asking you all to – I did not want to lose her comment. It was a fix that I was struggling with. I am good.

Rich Landen: We have the placeholder there. I think it is going to require more thought than we can give it at this second because we are naming organizations and then all of a sudden, we throw in data systems. There is a bit of a non-sequitur. But thanks for capturing that and again by extension, thanks to Alix Goss for submitting that suggestion.

Other questions or comments?

Rebecca Hines: Just to confirm, Jacki, we will do the update after the public comment later today. Is that your thinking? Would that make the most sense?

Jacki Monson: Are you referring to the update on standards.

Rebecca Hines: Yes. The ICD, the other things that are in that other slide deck.

Jacki Monson: Let us do a time check here. What time are we scheduled to start the --

Rebecca Hines: We are scheduled to start the PCS Cybersecurity Panel now. And then we have a public comment at four. And then we basically have 45 minutes after public comment.

Jacki Monson: Let us do that if that is okay with Rich and Denise. If we finish the panel early, obviously, we can start the update earlier.

Rebecca Hines: Very good. For anyone in the audience who is waiting for that update, it is going to happen after the 2 o'clock panel and either before or after the public comment period.

Maya Bernstein: I see that all panelists for 2 o'clock are present – participants.

Subcommittee on Privacy, Confidentiality, and Security

Jacki Monson: It looks like we are ready to go. Let us go ahead and move into the next agenda item, which to get an update on the recent issues on cybersecurity. As many of you know, over the last year, we have spent a lot of time in the cybersecurity landscaping, conducting a new evaluation as well as writing a letter of recommendation to the Secretary with respect to our recommendations on cybersecurity enhancements that would benefit patients.

It is my privilege today to moderate a robust set of panelists who are very well qualified, and we are lucky to have them today to share with us on recent issues in cybersecurity and provide us some updates since the last time we had an update, which was almost a year ago now actually to the date when we had our last panel discussion on privacy.

Today, I have with me Greg Garcia, who is the Executive Director of Cybersecurity over the Healthcare Sector Coordinating Council. I have Andrea. I am going to apologize because I have no idea how to pronounce your last name. If you could get off mute and tell me how to pronounce it. I would rather not.

Andrea Matwyshyn: Matwyshyn.

Jacki Monson: I would never have guessed that. Thank you very much. She is a JD, PhD, Professor of Law and Engineering Policy at Pennsylvania State University.

And then we have with us Reuven Pasternak, who has been with us before. He is a physician by trade. He is the Senior Advisor for the National Risk Management, Cybersecurity, and Infrastructure Security Agency.

And then we have Linda Ricci, who is the Director of the Division of All Hazards Response Science and Strategic Partnerships, Food and Drug Administration.

We did invite NIST, and they were unable to join us today.

With that said, let us go ahead and get started. Greg, I am going to ask you to kick us off. Each panelist will have ten minutes to provide a presentation and get us an update. And then what I would like to do is let all of the panelists cover their information and then we will open it up for Q&A afterwards. Time is a little flexible, Greg, if you want to – 10 to 15 minutes, I think, will be sufficient.

Greg Garcia: I will keep my slide deck if everyone can see it off of presentation mode and in editing mode just because it is easier for me to just jump ahead. I do not want to go through every slide if that is okay. Are the slides large enough for you to see?

Jacki Monson: You zoomed in a little bit and it is hard to see the whole slide.

Greg Garcia: I will zoom out a little bit. First of all, thank you for the invitation. I appreciate being here. Just a quick overview of me. I have been in this role now since 2017. My background is mostly an industry guy but sometime in government, I have spent with the Department of Homeland Security. I was an Assistant Secretary under the Bush Administration and Department of Homeland Security, running the National Cybersecurity and Communications Strategy and have also been in the financial sector with Bank of America and the Financial Services Sector Coordinating Council. There are 17 sector coordinating councils I will go into in a moment. I have also stood up the IT Sector Coordinating Council. I have spent time in the Congress associated with a piece of legislation called the Cybersecurity Research and Development Act of 2002, which is intended to build the Cybersecurity Workforce Pipeline through the academic community.

Let us just start with the basics. We are a critical infrastructure. Just like 16 other critical industry sectors, financial services, electricity, oil and gas, water, transportation, communications. This is all enshrined in not just the Patriot Act but a series of executive orders that call out the critical infrastructure partnership between industry and government, public-private partnership.

This is called out – all the sector coordinating councils are actually federal advisory committees like NCVHS with the exception from FACA requirements regarding public disclosure, inviting public to our meetings because we are dealing with sensitive, critical infrastructure, threat vulnerability and mitigation information that is not something that should be in the public domain to make us a target.

That exemption is called CIPAC, Critical Infrastructure Partnership Advisory Council. It simply allows these industry organizations specifically and exclusively the sector coordinating councils to work with the government on an ongoing basis. And indeed, Reuven Pasternak and Linda Ricci, who you will be hearing from later, are active in our sector coordinating council. But to work with government on an ongoing basis without those FACA requirements, with a couple of exceptions. One of them is we cannot charge dues. It is not pay to play. And secondly, we do not lobby the government. We are an advisory council and you all understand that distinction.

If we do not charge dues, how am I here? We do accept contributions, donations from member organizations on the industry side. The Health Information Sharing and Analysis Center, the H-ISAC, actually made the decision to hire me as a full-time salaried executive director to manage the cybersecurity working group. I am fully on the industry side and that is the essence of the public-private partnership that we have.

The Industry Sector Coordinating Council and the Government Coordinating Council working together on an ongoing basis to identify and mitigate these systemic threats whether they are natural threats or manmade threats like cyber-attack.

And of course, when we look at the health care ecosystem that we are representing, this is a pretty good schematic of it. You all may recognize this coming out of the health care industry, cybersecurity task force. You mentioned this in one of our documents that I read through, which I thought was very good. But the Cybersecurity Working Group, the Health Sector Coordinating Council represents pretty much all these sub-sectors, recognizing that we are interdependent and interconnected in many ways. We need to address those issues that are cross cutting in nature.

Again, this is looking at Presidential Policy Directive 21. It is just the most recent in a series of these executive orders, dating back to 1998. That really provides not a mandate or a regulation on industry. It is more of the directive from the White House to the federal agencies that have principal responsibility for these given critical sectors to work in that partnership framework based on the recognition that market forces alone are not going to solve these complex, evolving, cybersecurity problems. And regulation alone will not solve these problems. There needs to be a more innovative and resourceful way of dealing with these issues.

The Cybersecurity Working Group is the largest standing working group. We are co-chaired by industry and by government partners. At the bottom of this slide, you see HHS ASPR, the Office of the CIO, and FDA.

This is our membership now as of the end of last month. Again, these 300 – almost 320 organizational members span the various subsectors, medical devices, direct patient care, plans and payers, health IT, pharma, labs and blood, public health. We do also benefit from a number of advisor organizations, consulting firms, law firms, security companies that are not specifically health care organizations. But they do have the expertise and the thought leadership to help us out pro bono, provided they are not doing any business development. This is not a trade show.

And of course, big force multiplier in our membership are the 45 increasing industry associations that have that much broader platform. And of course, we have a number of government agencies. When we come together, we are the joint cybersecurity working group. We have federal, state, and local and more than 750 personnel representing that whole membership. This is just, of course, our membership distribution. Naturally, the direct patient care, the health provider organizations make up the lion's share of the organizations in the membership. Basically, how we are organized.

Like a lot of any organization, we have a charter with a governance process on the industry side. We have a vice chair and a nine-member executive committee representing the various sub-sectors. The Executive Committee members are elected by the general membership and the chair and vice chair are elected by the Executive Committee.

Down here, you will see another slide that is a little bit larger. These are our active task groups. I will go into what these task groups are about. This is just our Executive Committee. You can see a fairly senior executive group, representing the various sub-sectors of the health sector. It is really important to have that cross-sector perspective because we are all dealing with cyber threats that are similar in their approach but often different in their impact. We need to take that into account and some of the differing business models and the interdependencies as we work through some of these complex problems.

Again, these are our co-chairs on the government side. We meet with them every Friday as well as representatives from DHS, CISA, and sometimes others to just make sure we are coordinated, synced up, no surprises so that we can better and more effectively address the joint chair challenges we face.

I mentioned the Health Care Industry Task Force. As you all acknowledged in your report and the May letter to Secretary Becerra, this is our guiding compass. This is the 2017 report. HHS established this task force at the direction of the Congress. About two dozen industry and government experts in cybersecurity and health care were told to answer two questions. Why is the health care industry getting hit so hard with cyber-attacks? And number two, what do we do about it? Their determination was of course that health care cybersecurity is in critical condition for the reasons you see there.

What we did is – and then they come up with the six major imperatives for what needs to be done. And under those imperatives, the cascade, about 105 action items so very specific action items, which we in turn starting in 2018 after we had reorganized when I came in, we established a number of task groups. Cybersecurity function-specific task groups, like how do we improve cybersecurity controls and hygiene in the clinical environment. What about medical devices? How do we design and develop and build cybersecurity and medical devices from the ground up? What about workforce, research and development in the pharmaceutical industry? How do we protect the crown jewels? We establish task groups.

Let me jump ahead to those task groups and I will come back. Task groups are made – are established to form, do their work, and then fold unless there is a Version 2 or something that they need to continue working on. These are not in perpetuity. But these are the standing task groups as of today with the ones in the box being the most recently established in 2022. I will not go into what each one of these is about. Some of it is self-explanatory.

But our primary focus has been simply trying to raise the bar across the entire ecosystem of the health care industry particularly the small and mid-sized organizations that do not – they know they have a problem, but they do not necessarily have the resources or the expertise of the technology to deal with these problems.

We bring together these task groups made up – chaired by different sub-sector organizations, made up of anywhere from 42 to 140 people, bringing to the table some of their best practices. We are talking about some of the larger, more resourced organizations from the various sub-sectors, who have invested a lot in cybersecurity and understand the nuances. And they are bringing their best practices to the table that we integrate and then publish for the benefit free of charge to the rest of the community. Since January of 2019 at the bottom here up until May 2022, we have produced best practices guidance documents for the benefit of the sector, by the sector, for the sector. These address most of or a lot of the recommendations coming out of the Health Care Task Force Report that I referred to. All of these are available on our website at healthsectorcouncil.org. It is actually now called the publications, not recommendations. These needs to be updated.

But here, we simply have mapped out how each one of these HCIC imperatives, task force imperatives, is addressed by the deliverables, the publications that we have offered up and when it was delivered. That is just a performance assessment in a way.

Our biggest issue now in going forward is how do we ensure that we get these tools in the hands of the stakeholders who need them. For want of a better term, it is marketing exercise. As a nonprofit, non-budgeted coalition of volunteers, this is a significant challenge. We will be relying on HHS and other of our members to be the force multipliers to drive these tools into the community and at least at a very rudimentary level, we are measuring downloads of views and downloads on our website as we publish them. I imagine these numbers are much bigger when you think of the number of trade associations and other ambassadors who are pushing these documents. And then we have a number of them on deck that will be published over the next couple of quarters. There is still more to come.

What we have been focusing on now is not just the marketing part, but we recently had a meeting with the National Cyber Director in the White House, Chris Inglis, who has been particularly drawn to the work that we have been doing as a model. His ask of us as it is of ourselves is that this task force report now is five years old.

What has happened in the health care industry over these past five years? How has the industry changed the business models and subsequently how has the threat environment changed? Which of the many task force recommendations have we successfully addressed or at least made progress? What remains to be done? What does health care cybersecurity look like five years from now and how do we organize ourselves toward getting to that point? They are all very difficult questions. We will be spending a lot of time over the next year or so developing that next five-year plan.

At that White House meeting with Director Inglis, there were also senior HHS executives there who made personal commitments to ramp up the HHS partnership resources, authorities, and capabilities to ensure that the Sector Coordinating Council and related organizations like the Health-ISAC are doing this truly in partnership that we pool our resources, our thinking, and our strategies because this is – one of Chris Inglis' most off-quoted lines, which is very compelling, is you have to beat all of us to beat one of us. That is sort of a riff on three musketeers. But that is really what we need to be focusing on.

I will stop here and just encourage this Committee. I really appreciate the attention you have put onto cybersecurity. I think the recommendations and the letter to the Secretary Becerra are on point. I think from our standpoint, we are probably wanting to get more aggressive with HIPAA, which is a truly outdated law, particularly when it comes to cybersecurity.

We have tools and frameworks that we think taken together serve as a pretty effective reference point for the health sector that takes us well beyond the HIPAA Security Rule and takes us into more operational guidance that would ensure HIPAA Security Rule compliance.

I will stop there and look forward to the Q&A.

Jacki Monson: Thank you so much, Greg.

Andrea, do you want to go next?

Andrea Matwyshyn: Sure. I would be happy to. Thank you very much for inviting me to join you today. I thought I would throw up a few words just on my background. Some guideposts for a few comments that I will make. Unlike my esteemed co-panelists, I am the cranky professor in this space, who has a bit of a more removed view. I have the pleasure of working with multiple different agencies on issues of security. To that vein, I need to disclaim that any comments that I make today, I make in my personal capacity, not in the capacity of representing any agencies to which I may be currently appointed.

I am a law professor, an engineering professor at Penn State. I run two labs, both of which focus on technology policy and human life betterment. I have been studying questions of security since the late ‘90s, first as a corporate lawyer and then an academic.

I would like to share a few observations about where I see security going in health tech spaces. You will notice that I said health tech rather than medical spaces, because of the creeping convergence of various different dynamics in our economy that make interdisciplinary approaches across agencies and cooperative efforts all the more critical. I will flag four bunches of issues and I will be brief and hopefully stimulate some thoughts perhaps for our later discussion.

The first point that I would like to share is the recognition that is not yet universally shared across the private sector or across agencies that questions of confidentiality, integrity, availability in the security sense are issues of safety. And that without a robust approach to security, patient and consumer safety is unfortunately not achievable.

I flag this partially because I see a repeating conflation particularly among privacy attorneys between the privacy notions of confidentiality and the security notions of confidentiality, which are slightly different, both important and complementary, but nevertheless, on the legal side, I see that. But meanwhile, in particular, thanks to some research that some medical school students that I was supervising in graduate work this year that it has become unfortunately obvious that medical school curricula are not training our future doctors on the basis of these security principles and the ways that technologies can impact patient safety very directly.

As we think about how to work across sectors and across agencies on these issues, these education questions about bringing relevant professions along to help in being the dispersers of the good ideas that we come up with, that, I think, needs to be a part of our conversation on these issues. That is the first point that I would like to flag, that education point.

But looking more broadly at where we are going in questions of security and health tech, we know of the rampant vulnerability that has permeated the Internet of Things. We know of the nightmarish botnets. We know of all of those dynamics that have now started to creep into hospital context and to medical context. Thankfully, medical devices are becoming progressively more safe thanks to the hard work of the FDA, which I consider to be the leading agency on security as far as consumer outreach today. But nevertheless, the FDA's thorough position is not yet shared across government and various consumer safety contexts.

These questions of the Internet of Things – vulnerabilities transferring into health tech devices leads to another layer of mess because these are not necessarily all medical devices. These are body attached, body-embodied devices that are talking to each other, to back-end systems, to machine-learning systems that are then creating derived data sets about the human bodies that are attached to those devices. While some of that ecosystem involves medical devices, some of it, as I said, does not. That means that the way that we think about ensuring baselines of security in these devices and to make sure that not only the medical devices have these baselines of safety but the other components in the non-medical device health tech, body tech, internet of bodies' devices, get that same level of robust analysis. That means that it needs to be across agency effort, which does not yet exist as robustly as I would like to see.

Now, the next step beyond this is that these devices that are attached to or embedded in our bodies are going to increasingly interact with the built infrastructures of our physical environments. We saw a little bit of a preview of this when we were experimenting with the COVID notification apps and you had someone in physical space with a phone that was invisibly identifying itself in relation to other phones with a set of back-end information about the human bodies that were ostensibly holding those phones.

But what we see in the private sector is that employers in the public sector and the military – we see that human bodies are increasingly directly interacting with these built structures. Some employers are putting chips into their employees for ease of security access to physical places or for free smoothies or for logging into systems. The chip that is embedded in an employee's arm – we do not think of that as a medical device but yet it is beneath the skin, and it is serving a non-medical function. But these are these sorts of devices that will be blended among the various potentially transformative lifesaving and life-enhancing medical devices that are similarly going to rely upon these internet connections that footnote may or may not be optimally stable to support them.

These questions of human bodies' safety becoming increasing reliant on the security of these health-ish technologies and the integrity of the information in the backend systems that are communicating about them – I am calling that the intelligent society problem that we are building this world where there will be a perception of a high degree of trust among these various data streams and devices and the security among them but yet the reality is of course that the attacks are becoming progressively more severe, progressively more effective at scale. Human bodies will be very attractive targets both in military context and in consumer and patient context.

We see the progressive mingling of national security and commercial security questions. Security questions are reciprocal and dividing out the traditional sectors that we might have done otherwise legally at least in the past becomes impossible in the same way. It is because of course it is the vulnerable code and the exploitability of that code and the existence of the flaws that lead to the possibilities for attackers to exploit.

Just to wrap things up and leave a bit of a concerning pin in things and a frame to think about, I am deeply worried about the arrival into our marketplace of multiple function devices. The 21st Century Cures Act specifically enables the development and deployment, I would say, though that is not quite how health technology creators might discuss it. But the commercialization and widespread adoption of devices that start out as health-related devices, medical devices. But then they also may have additional functionality that is not strictly speaking a medical functionality.

The 21st Century Cures Act leaves a lot of wiggle room for those non-medical functionalities to co-exist in ways that could end up being troubling from a security standpoint. Of course, because we know that any device in any system is only as secure as its weakest point, these non-medical functions could potentially be used as a point of lateral access into other kinds of functions in the device, depending on the build, and potentially cause physical harm to human bodies.

The world that I fear is a world where there is an embedded brain device that perhaps also streams movies directly into your brain and that non-medical functionality is not vetted thoroughly for the security of its coding. As a consequence, we have writing to human brains through these technologies that are explicitly created in some cases to allow both reading and writing. You have live data flows, both directions, attractive targets, and particularly depending on the incentives of the attacker, a potentially set of catastrophic events.

While it may be neat to be able to watch a movie in your brain, this also raises a set of questions about whether we have a shared vision of the direction of "progress" for the way that we want our health tech ecosystem to be built out for the betterment of our society. I think we need to have that conversation about the big picture goals of what we are building and why because there are many worst-case scenarios where this all ends very badly.

This is the time to think through where the stopping points can be, should be, what buffers we need to put in to ensure that the worst-case scenarios that can be easily threat modeled do not come to pass and to ensure that we have the betterment of human lives at the core of our analysis, not the generation of shall we say maximize shareholder value particularly in the context of the multiple function devices that will become progressively more common on the market in the near future. We are seeing the first rounds of those starting to arrive already.

I will leave it at that with that plea for the big picture discussion of progress and what we mean by it. And I look forward to discussion and questions.

Jacki Monson: Thank you very much.

Reuven, do you want to go next?

Reuven Pasternak: Thank you for the invitation to be here. I am lucky to follow Greg and Andrea because they have already covered a good deal of territory. I am going to be uncharacteristically brief. But I have a few slides that I would like to have up on the screen please. I will not be showing them myself.

While they are coming up on the screen, a few words about CISA, the organization that I am with and my background. First of all, my background is – I am an anesthesiologist and critical care physician. I was in the private sector in academics for 20 years and then went into health administration. I was a health care executive for another 15 years and also was in the academic side doing research and health systems risk analysis from both the scientific and operational perspective.

I stepped down from those roles in 2019 and handed over the reins to my COO and she promptly inherited COVID six months after taking over. She still has not forgiven me for that yet, but she did a marvelous job.

With that, I came in as the CARES Act was developing in June of 2020 and my role has been as somebody with a private sector background, straddling both the government side and the private sector side and doing that for two years and then two weeks ago, being asked to stay on full-time basis.

The manner of the work I am going is not so much the technical aspects of cybersecurity as much as it is areas of resiliency and health care. We are transitioning now from efficiency to resiliency as the buzzword of what we are looking to do. I am doing that in the context of my role at CISA, which is the youngest of the federal agencies, probably the fastest growing of the federal agencies. It is part of the Department of Homeland Security, currently headed by Jen Easterly, who celebrated her first anniversary in that position this week. In fact, I am missing that celebration now by being here. I got a special – for that one. It is a group that is still very much in the process of organizing and coming to – what has been an extraordinary challenge.

In that regard in terms of where we are at today – as Greg mentioned, we cover a broad front of activities. It is not just health care although health care is the largest of all the sectors in which we are engaged and probably has the most advanced cyber activity and depth of experience of them all.

But as we look at the broad landscape in which we are working in which we are concerned, the interconnection of everything in the economy and everything we built here makes this a concern for us. When a cyber breach occurs in a pipeline in Texas or with manufacturing plant in Washington State, the issue that arose there can be an issue that comes back to health care. We have to be watching across all these sectors, what is happening – the factors that are doing it, what are the methodologies that they use and then can this come back and get us into the health care sector. It is a broad range and a broad landscape with which we are concerned as we move forward.

When we look at the 16, we also break those down to national critical functions. It is very small print. I apologize for that. But three of the 55 functions in health care maintain access to medical records, provide medical care, and support community health. Again, the combined health care component is by far the largest grouping of issues and the economy that we have of any group in there and that includes defense and other areas as well.

Health care has a huge presence in this discussion, and it has a huge presence in this discussion because it is the most conspicuous target right now for cyber-attacks. It is the most conspicuous in cyber-attacks for the number and scope of the request that are being made and compromised of patient data.

As we have experienced the acceleration of cyber attacks over the last couple of years, we have encountered several challenges that we are looking to meet and as the agency has been growing and maturing these relationships having to deal with these as well.

And one of them is the cascading impact of disruptions. Andrea made mention of the fact that cybersecurity is not just an operational threat. It is a threat to patient safety. It is a threat to staff safety. When it occurs in one institution or one organization, it has cascading effects across the entire region.

You will see that in the green areas to the left, everything is operating functionally well. It is able to absorb more volume and perform all its functions. When a disruption hits a smaller unit or hits a medium-sized unit, it has repercussions for the other units in the area and can rapidly progress to involve a region-wide and even potentially nationwide disruption of services.

In the area of cyber, this is even more acute than it is in other areas of disruption for hospitals because in cyber, you do not get a several-day warning that it is going to come. It can come at any time of day. It can and usually is opportunistic to come at a time when it causes the most disruption and also leaves a hospital in a position and a health system in a position where it has the least capacity to absorb what is going on without having to consider giving whatever is needed to get back on its feet again.

In looking at the extent to which there is disruption in the organization, one of the challenges we have had is getting our arms around what is the impact of cyber attacks on health care systems and health care institutions. We have seen everything from small disruptions of operations to now state actors or large mature actors, bringing down entire systems for extended periods of time. And when they do that, as we said, it is a safety issue for staff. It is a safety issue for patients. In a template and I will be glad to send this out for those who would like to have a more easy to read copy of this, it is developing as a one through five system where one level system is or a system that is fully operational as high resiliency, able to absorb additional capacity. Two, it is where it is working well but is low resiliency, cannot absorb much more on up to three, four, and five with five being the point where a health facility literally has to close because it has been brought to its knees. It has happened with hurricanes, and it has been at risk of happening with cyber.

The extent to which this can happen even in very sophisticated systems can be rapid and decisive. In one system in a metropolitan region with four million people, one of the three primary systems was hit and within a 24-hour period, one-third of the ICU beds were taken out of use in that system, entire specialty units were out.

This is the sort of activity that cyber intrusion can have in addition to the compromise of patient confidentiality, in addition to the financial compromise that comes to the organization. The imperative for being able to know what is happening as quickly as possible is there. And for the hospitals and the health systems to have the resources that they need to be able to address it and to be able to prepare for it and to have the support that is needed to make themselves resilient and to anticipate this threat coming.

There was a time a couple of years ago when these episodes would take several days to track down and get resources coordinated in the government. Over the last couple of years, that has improved significantly to where we have the FBI included. The SRNA, which is Health and Human Services and also CISA involved so that the agencies are coming together to work on a more immediate basis needs more improvement. But being able to have a coordinated federal response, as, I believe, Greg may have mentioned, is critical to the success of moving forward and being to mitigate these risks and doing this in concert with the private sector that is rich in experience, rich in expertise, and rich in enthusiasm for making the situation better and improving the security platform of this country moving forward.

Finally, we have competing for attention. As we are talking about the digital platform -- I call it the Digital Commons because we are sharing this Commons with many people besides health care and health systems and not just hospitals but public health clinics, any place where patient care is being provided – is facing the challenge of finances, is facing the challenge of facilities in disrepair, staffing challenges, supply chain issues, quality and safety, and is also facing a challenge that we are finding especially to a number of us, the fragmentation of the system whereas before you could find your entire constellation of activity within a very closed system, sometimes a single building or under an administrative aegis now scattered over the landscape and involving many players with differing resources and attention to cybersecurity and cyber platform and how you bring those all together and ensure the safety of patient data and ensure the safety of patient care. The last one is digital platform and cybersecurity.

And the last point I will make echoes something that Andrea said, which is that cybersecurity now is where quality and safety were 20 years ago. Twenty years ago, quality and safety were recognized as important, but it was an afterthought. It was an afterthought in the education and training of our people, and it was an afterthought in terms of how we resourced it. And over 20 years by hardwiring it, by building it in to be part of the system and recognizing that everybody has to be engaged with it and one person not being engaged can have catastrophic consequences. We need to in our many cases moving into that area as well.

One of the groups that Greg has talked about and he had it up on the screen is precisely the one that Andrea mentioned. Training people. How do we train our workforce of the future to make them mature enough to be able to appreciate cybersecurity and implement those and that is a lot of the work that that group is doing as well?

There is so much more to be said about this but I am going to hold there and wait for Linda to speak and then look forward to a robust discussion after that. Jacki, back to you.

Jacki Monson: Thank you so much.

Linda, are you ready?

Linda Ricci: Thank you very much for including me in this discussion today. My co-panelists have covered a great deal of the material that I was planning on covering as well. I will try to make this brief and cover the highlights.

My name is Linda Ricci. I work at the FDA within the Center for Devices and Radiological Health. I work in a group that has a diverse portfolio in the Division of All Hazard Response, Science and Strategic Partnerships, part of which is cybersecurity policy for medical devices. Medical devices are a critical part of the health sector ecosystem and as such, as have devoted time and energy and resources to creating those guidances that are needed to help manufacturers produce and maintain devices across their life cycle to be cyber secure.

I am going to go back a little bit, take a step back and just to level set. I am sure we are all aware of this but I am not sure that we can talk about this enough. Cybersecurity flaws lead to unavailability, unavailability of health care records, unavailability of meat processing plants, unavailability of Vaseline in a pipeline and unavailability of medical devices.

I think it is important to point out that there have been companies recently that have been hit with old ransomware. While we are trying to deal with ransomware that we have seen before, the threats are forever getting more and more sophisticated.

This article came out earlier this year that there was actually a group of Russian-affiliated cyber criminals who were looking to attack hospitals in the middle of the pandemic. Going back to the discussion that Reuven started about if you have an attack on one institution and what that does to diversion of patients, imagine if there were a state sponsor or even if it is not state sponsored that then becomes less important. But if there is a coordinated attack against areas of the health sector such that you get to the last stage in Reuven's diagram and you have no space to divert patients, you have no ability to care for patients. Then that becomes a real problem for everybody obviously. Some of these groups are looking to instill panic and really make an impact on our infrastructure.

What are we going to do about it? FDA, as I indicated, and CDRH specifically, is very focused on medical devices. That is our oversight, and it is our mandate. We have prevented devices coming to the market based solely on cybersecurity concerns. This has been through our pre-market processors. There is a number of different pathways that a device can get to market based on the risk of the device and we have been able in certain circumstances to prevent devices that do not have adequate security from getting on the market.

This is important because it helps devices not become legacy devices of the future. We want devices before they go on the market to have the adequate cybersecurity and be able to maintain that cybersecurity across their life cycle.

This is important because cybersecurity is safety. CDRH has a mandate of providing reasonable assurance of safety and effectiveness for medical devices. We see cybersecurity as part of that patient safety and a lack of cybersecurity in a device that allows that device to be hacked and impact the hospitals, that allows that device to impact the patients directly. That becomes a safety issue.

To help our industry with creating devices that are cybersecure, we have a number of guidances. In 2014, which honestly when every time I read this, I cannot believe it has been almost 10 years, but I know we have all the past two and a half years. But a long time ago in cyber land, we developed this premarket guidance. This premarket guidance really was one of the first guidances for the agency that spelled out that cybersecurity is important. Cybersecurity needs to be addressed in premarket submission. And that devices before they go on the market need to have demonstrated cybersecure aspect to them. They need those characteristics of security.

This is followed in 2016 when we finalized the post-market guidance. Now, pre-market is only the first half of this. If you create a device and it is cybersecure when it goes on to the market, we all know that that device will not necessarily stay cyber secure. We expect devices to be able to be patched and updated. We expect manufacturers to monitor for vulnerabilities so that device can maintain its security across its life cycle. This post-market guidance covers our expectations for what manufacturers will do in the post-market.

In 2018, we drafted another pre-market guidance. It had a lot of feedback on it. As a result of the feedback, we revised that draft and have republished that in draft just this April.

A little bit more specificity on this guidance. It was published in April, as I indicated. The comment period just closed about two weeks ago. In terms of what changed from the 2018 draft guidance, there are more detailed technical recommendations. We did remove some risk tiers. We believe that all devices need to – if they have software, they communicate externally, they need to demonstrate cybersecurity. However, we do understand that that documentation may scale with the cyber risk provided by that device.

We also included detailed recommendations for Software Bill of Materials.

We also have proposed some legislative action for medical device cybersecurity. While we have a broad mandate for reasonable assurance of safety and effectiveness, there are no specific statutory requirements that expressly require medical device manufacturers to address cybersecurity. We believe that with additional expressed authority to mandate cybersecurity, we can do a better job of protecting ecosystem and keep devices cybersecure.

Specifically, in our A-19, we have discussed the Software Bill of Materials. We have talked about that devices need to have the capability to be updated and patched in a timely manner. We have indicated that manufacturers need to demonstrate reasonable assurance of the device's safety and effectiveness specifically for the purposes of cybersecurity and that manufacturers should have coordinated vulnerability disclosure policies that allows them to better manager cybersecurity vulnerabilities publicly when they happen.

Just a few device cybersecurity highlights. One thing that is different about medical devices is that they are an operational technology rather information technology so OT versus IT. We have seen that the threats to OT are continually growing. This can result in supply chain risks that can extend significantly beyond CDRH medical device domains.

We also recognize that OT cybersecurity is inherently a shared responsibility. There has to be coordination across the government sectors and the private sector. We have been able to coordinate certainly within CDRH but across HHS with DHS and NIST, with private sector through groups such as the HSCC that we heard about earlier today with Greg with security research firms, with trade organizations, with physician societies. We recognize that the continual need to have this coordination because it is a shared responsibility.

Our team within CDRH has taken a total product life cycle approach. It is not enough to make sure that a device is secure at one point in time before it goes on the market. This is a life cycle approach that needs to be taken to make sure that devices can be managed in the post-market, can be updated and that will help the medical device ecosystem itself be more secure.

I also want to point out that we did pen a response to a NIST request for a comment on their workshop that they had for standards and guidelines to enhance software supply chain security. Our response really wanted to highlight that there is a difference between IT and OT and it needs to be recognized. Both are critical and both need to be secured.

And the critical functions for devices are no longer in necessarily a single box but we have distributed technologies that are performing the OT function. It is becoming complex and definitely needs attention.

Lastly, I want to end with just a few resources that we have helped to develop through the ecosystem. The first one is a shout out to Greg and his group with the Joint Security Plan as he highlighted earlier. There are a number of documents that have been generated through the agency and fantastic resources for the ecosystem, not just medical devices, but certainly medical devices benefit from these resources that are available.

We have also worked with MITRE and MDIC to create a playbook for threat modeling medical devices. We recognize that threat modeling is an important tool in helping medical device manufacturers understand the threats associated with their device and be able to build in mitigations to respond to those threats. This threat modeling playbook is intended to help educate the ecosystem with regards to threat modeling.

We have all used the NTIA SBOM documents that have bene produced. In addition, we have worked with our international partners through the International Medical Device Regulators Forum or IMDRF. They have a created a number of cybersecurity documents that are intended to work across the globe for medical device cybersecurity. If we can agree in a global sense about how to secure medical devices then it allows for there to be seamless introduction for products across the globe and makes the job of securing them a little bit easier.

Lastly on this slide but certainly not the last resource we have developed, we have developed a Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. This is intended to support regional incident responses that involve medical devices.

Just in summary, cybersecurity is a big task. Cybersecurity for the health care sector involves everybody and we all need to work together in order to protect this critical infrastructure. FDA and specifically CDRH understands the need for medical devices typically to be secure in order to help the overall ecosystem be secure and we continue to work with other governmental partners to understand where there are gaps and how we can best use our oversight into medical devices to help build those gaps. Thank you.

Jacki Monson: Thank you very much and thank you for all of FDA's work on SBOM and everything else that you are doing. You are certainly leading the path to helping from a cybersecurity standpoint.

Let us go ahead and open it up to questions from members of the committee. While we wait for them to raise their hand, I will just keep asking questions. The first question to all of you – you have seen the work that we have done, the letter of recommendation. From your perspective, what else can NCVHS and the Subcommittee on Privacy, Security, and Confidentiality do to support this effort and work?

Greg Garcia: I will start. I would say that your work is complementary and supplementary to what we are doing in the Sector Coordinating Council. I saw also that you recognized the work we did in your letter to the Secretary. I would just say keep doing that. Refer to our resources. Encourage HHS and the various operational divisions to – I know there is a fine line. You cannot say endorse certain industry products unless they are co-branded. Linda brought up the joint security plan, not so much co-branded, but co-developed.

Since we are a partnership, an official partnership under Executive Order, we do rely on our government partners to provide that force multiplier to the broader community and to drive these resources out to the community and to think creatively about policy proposals that could not make the sector more secure and resilient.

I think of the law passed last year, Public Law 116-321, which actually called out one of our work products, which is co-developed and co-branded with HHS called HICP. It is called HICP, the Health Industry Cybersecurity Practices, which is sort of the top ten cybersecurity controls that a clinical enterprise needs to deploy. And in that law, there was the directive to OCR when enforcing a HIPAA data breach to consider the extent to which the breached entity had over the past year implemented the HICP done by the Sector Coordinating Council and HHS, the NIST Cybersecurity Framework or other "recognized security practices". Having that statutory recognition of what we are doing and the impact on the sector is particularly important.

Another example is I was asked to participate on the Technical Advisory Panel of the Joint Commission, which was responding to the OIG report from last year that recognized that CMS was not paying particular attention to the security and the security management of medical devices in a health provider. The Joint Commission is exploring the extent to which CMS can use its reimbursement authority as an incentive for better cybersecurity risk management for medical devices. But I think that can also be expanded into other areas as well, provided at least in the transition, it does not impose too heavy of a burden on those smaller to mid-sized institutions that are struggling under the weight of solvency concerns and pandemic pressures.

Those are a couple of ideas that the committee, I think, can get behind, as well as continue to think about how do we enhance the workforce, bring in better cybersecurity talent into the health care industry, and also do better training of the clinical workforce about their responsibilities in cybersecurity.

An example for workforce could be student loan forgiveness for STEM and cybersecurity grants if they were to join the health sector. Of course, the health sector competes against other very well-healed industry sectors like technology and financial services. It is a dog-eat-dog world when it comes to recruiting cyber talent. Whatever we can do to and recommendations you can make to encourage those kinds of incentives. I have other recommendations similar to yours, but I will stop there.

Jacki Monson: Linda or others, do you want to comment?

Linda Ricci: Just adding on to Greg's excellent comments is really just keeping the pressure up. You should expect that health care systems be cyber secure. You should expect that medical devices are cyber secure. Yes, things happened. Vulnerabilities will happen but they should be recoverable. Keeping the pressure up to say that this is a key issue. This needs to have national attention. We need to have the workforce. We need to have across the sector the appropriate budgets to manage this because it is a critical issue for the whole ecosystem.

Andrea Matwyshyn: Just a few quick add-ons to Linda's excellent comments. I noticed references to playbooks and the recommendations. There is a threat modeling playbook that is new out from MITRE that would be potentially useful to point organizations to. It is dealing with health devices in particular.

DOJ has guidance on baselines of corporate conduct to help make organizations more resilient to attack. All of these organizations that are creating health products, health devices, health systems, there are also structures of corporate governance in themselves. That CCEP's guidance on the way that companies can make themselves more resilient would be another document to maybe connect with. Similarly, ISO 29147 and 30111, which deal with building internal structures for vulnerability intake and management and external communication with finders because of course sometimes things get discovered when they are already out there, and companies need to learn from those mistakes and be ready to intake information and iterates their products to make them even better.

And the last one that is my blue-sky idea, I would love to see some sort of funding that is allocated for medical professional curricular development, perhaps through either CDC or HHS through whatever office is appropriate to help medical schools engage with the technology issues around security that are currently completely absent from the curriculum.

And similarly, CDC has some creative programs for training up people to be skilled practitioners in epidemiology or dealing with pandemic response. We could create that kind of a program for dealing with security response. Perhaps the way that we trained up a core of health responders to deal with earlier pandemics, we could launch a national program that is funded through CDC or other partner agencies to create a new core of quick responders for security emergencies particularly in health sectors. I will stop there. But those are some ideas.

Reuven Pasternak: My colleagues have done to cover it. I would like to turn this back. I know there are a number of people who are watching this who are in organizations that are dealing with this issue and perhaps ask if they have any thoughts about how we have responded and about how we may do a better job of providing the sort of support that people need to be able to deal with this issue.

Jacki Monson: It sounds good. We can certainly – I am sure we will get public comment on that particularly. Thank you.

Val, do you want to ask your question?

Valerie Watzlaf: Thank you, Jacki. And thank you, all, for being here. I really appreciate your comments. I think this is probably more directed at Andrea but it might be for all of you as well. Andrea, I just thought your presentation was so fascinating, especially I do not think I really thought about what you brought up about the embedded brain devices that are not necessarily directly used for medical care but could also be ones that are probably most vulnerable.

I guess my question is to you is how do you think these types of devices should be regulated or are there guidance documents. What do you think should be done in relation to those?

Andrea Matwyshyn: I have a paper called The Internet of Bodies. It is in William and Mary Law Review where I go through some of this. But the short version is that I am deeply concerned about any technology that allows for writing to the human brain in ways that could be basically create a false set of sensations for the human whose brain it is that the device is embedded in.

There is already a little bit of a phenomena happening where people are trusting the readings on their devices over their own sensory perceptions of self and of their well-being. That is starting to head in the direction of a form of almost device misinformation. I am worried about those dynamics particularly because it is a very attractive target for attackers and for using those access points for ways that are not in the best interest of the human.

For example, we know that the advertising ecosystem is very aggressive in the ways that different avenues to grab attention are deployed. In a recent public FTC meeting, there was a comment from a member of the public who works in, I believe, the advertising industry about her concern that devices and advertisers are figuring out when people are asleep and trying to subconsciously push advertisements into their awareness.

When you have a device that is live linked with real-time update capability and feeds into the human brain, the potential for uses and repurposing that the human who agreed to have this put in the brain thought of, the disconnect between what can actually be done and what that human understood is a matter of informed consent, can end up being tremendously divergent. And because all of these devices can be updated at any time by a remote third party, the possibilities for abuse are very real and concerning.

Honestly, I think the 21st Century Cures Act approach -- I understand where it was coming from but I think we need to rethink the permissiveness of multiple-function devices.

There is currently a default presumption in favor, absent a statement from HHS about the impermissibility of certain types of conduct. One way to go about this would be proactive statements about certain types of applications or uses that would be deemed abusive and not acceptable. That would be fantastic. I am happy to engage on what such a list might look like.

Or the other option is to flip that presumption in favor of greater evaluation for particularized changed uses and non-medical applications in light of the concern for human safety arising from even the non-medical uses of those devices.

Jacki Monson: Vickie.

Vickie Mays: Let me thank my colleagues for bringing this absolutely delightful panel together. My mind – it is almost like it is just racing. Thank you for that.

I have a question. It is a little bit like what Maya is asking. I am trying to really understand what are the real touchpoints for change and who should we be thinking about. Some of these seem to be outside of health and maybe even belong in Commerce for all that I know.

Let me just ask because – for example, NIH and NSF, for example, does all of the funding in research space for the development in health of a lot of these devices. Should one think about requiring that if you get research funding that you have to build in cybersecurity or is it that we should be thinking about the app stores where things are placed that they have the responsibility for doing that? Is that an IRB issue and that it should be checked to make sure that there is security at that level?

I did not hear you say anything about our schools of engineering. You are kind of going after our schools of medicine. But most of the time, we are in collaboration and following – we have the ideas and the vision. And some of the times we do not know everything that can be done and engineering really should be foremost in your minds for some of this. Can you help me understand what you think is really a government responsibility and what might be the responsibility of other areas in society for this?

Linda Ricci: I can certainly kick off for my thoughts on this. Because cybersecurity is such a shared responsibility, there is a piece of this for everybody. Yes, engineering schools need to as part of their curriculum and many of them do include – there are areas for cybersecurity. Computer science definitely has emphasis on cybersecurity.

I think one thing that at least we have found through how we are thinking about cybersecurity for medical devices is the remediations are often going to be different when you are talking about something that is life saving or life sustaining versus – like my banking apps. If there is a cybersecurity vulnerability in my banking app, a best engineering practice might be to take it down. I can wait and do my transfer later.

If you are talking about something in a hospital like a robotic surgery system that is in the middle of a procedure, how do you safeguard that and that immediate environment such that it can still function?

One of my favorite stories on this comes from Dr. Julian Goldman. You may know Julian. He talks about accessibility. If you have a set of drugs, for example, that are used in an OR and you want to limit availability of that drug, one thing you can do is make that – put them in a safe and make them only accessible for fingerprint. That is all well and good until you are in gloves in the OR and now your fingerprint -- you cannot get to the drug that you need for patient care.

Thinking about not only best practices because there are so many best practices that can be used to design medical devices and need to be reinforced not only in computer science but in biomedical engineering, for example, when you are thinking about how you – a device.

But you have to design for the purpose of the system. It is not safe to the patient for your doctor not to be able to get to a drug even though the drugs themselves are now safe from abuse.

There are some nuances that I see within the health care industry that perhaps are not as apparent in more of the general type of security landscape.

Andrea Matwyshyn: On the point of engineering schools, I could not agree more. The engineering schools have not incorporated basic security training in the foundational courses in most instances of engineering education. There is plenty to fix in every way. Most law schools do not have a course on information security. You have courses on health that do not have a section on device security. You have courses on bankruptcy that do not necessarily discuss the ramifications of data bases of sensitive health information being resold for the benefit of creditors instead of the benefits of the patients or the contract rights that issue into some of these devices. I am worried about a world where live feed rights based in contract can be shared among creditors because the bankruptcy courts' consideration is for paying off the debts of the startup rather than the bodies and the safety of the humans that are attached to these devices.

There is plenty of need for educational intervention can go around and I agree with you completely that the engineering schools are one of the core places for this to happen.

Reuven Pasternak: Vickie, I would add one level to all that has been said because I certainly agree with it. But I think what we have heard are also solutions that can be multi-year solutions and there are things that can be done now or should be down in dealing with cybersecurity. I think bringing this back to where the contact with the patients is occurring, where the health care providers are working with patients and having this become recognized as an immediate issue that has some remedies that are not hard to do that it does not eliminate the threat. But it does help the same way hand washing and quality and some of the others. That introducing some of those measures and having those being done on a universal basis and getting that into the mindset of people today that cybersecurity is a present problem. There are things we could and should be doing and do that in preparation with the other activities that prepare for a better tomorrow as well.

Greg Garcia: I agree with Reuven on that. I agree with the other comments as well as they are longer-term solution. But there are things that we can -- there are some basic issues of hygiene, which gets to training and, yes, workforce development. I think where the government can be helpful is trying to drive those incentives that –-

I think, Vickie, your question was what are the key touchpoints? The key touchpoints are the smaller to mid-sized hospital systems that cannot afford cybersecurity technology or to higher a chief information security officer and how do they do this.

By the way, someone coming from the financial services sector, I was with a top ten bank. But there are thousands of community banks around the country. We are in the same situation as small community hospitals. Their cybersecurity person is also their HR person. Only they are not a cyber person. They are an IT person. Our focus then in finance as it is here in health care is how do we – the rising tide lifts all boats. How do we get the smalls to the mid-sized organizations up to a minimal level of cybersecurity proficiency, which is not necessarily expensive? It is driving the incentives to get them to do that. It is carrot and stick of course. There is regulation but there are also incentives. The Public Law 116-321 is an example of that. Providing grants to needs-based organizations to join any of these collaborative organizations like the information-sharing analysis center or another ISAO, information sharing and analysis organization.

One of the fundamental tenets of cybersecurity is situational awareness. What is going on around you and what are others doing about it? How do we have this culture of you need to beat all of us to beat one of us that is not expensive but it is effective? We can help out that way.

I think the small and mid-sized organizations, given that we are all interdependent in so many ways, they themselves are a vector for broader impact throughout the health sector when they are vulnerable and unprepared.

Jacki Monson: Thank you.

Melissa.

Melissa Goldstein: Hi everyone. Thanks so much for this fascinating panel. You have made me think, which is very welcome, and I appreciate it, which was the goal actually for this fabulous panel.

My training is in law and bioethics. I teach in medical schools, schools of public health, and law schools. I have a mix of people all the time everywhere. Like the discussion that Vickie started about the difference in who do we train, medical students, engineering schools, all of the above, I am now thinking about cross agency, across the federal government and states laws as well. When we talk about regulating, obviously, HHS has a statutory purview and commerce has a statutory purview and the FTC also has a prescribed rule. And all of these are involved. All of these different agencies are involved in this work and our role, as advisors, to the Secretary of HHS. We obviously can recommend cross-agency work. Not mandate, not required. We can recommend it.

Andrea, your comments made me think a lot from the bioethics field in terms of dignity of the body, insults to the body, insults to ourselves, our flesh and blood, which is different than the exchange of "data" or information, which we might call it.

Now, that may not be approachable by any level of government except for use restrictions. Lorraine circulated – I am not sure if you all saw the idea of medical device software and where that can go or maybe mobile app software. I think, Lorraine, I misspoke.

In a way, this is the what should you be doing. It is not a mandate. It is the what should you be doing. Again, I would raise from Vickie's standpoint like even if it is a government purpose, a government role, shall we say, where should that lie? Who says that? An interagency and are they guidelines. Are they requirements? Is it a congressional level, which of course raises the level of complications required in getting it passed and then becoming flow down?

I am thinking about what are use restrictions, who are good actors. We can define that. We can sort of like what TEFA has said. Who are the good actors with ONC? And then what is the actual data? Data that might cross into that brain implant. Of course, this is all edging on science fiction.

Andrea Matwyshyn: Unfortunately, it is not. There are already patents --

Melissa Goldstein: Or an insulin pump. Information going in that causes a bodily injury, a personal harm, which would be covered by FDA. What about the information coming out from the various devices too? Is that FTC? Is that FDA? Where do you think our proper role is? We advise the Secretary of HHS. How would we craft those ideas?

What do you think is – obviously, these are all complicated multi-year issues. All of them. Where are the baby steps? Where are the certain steps forward that we can take? Essentially, these are societal decisions that we now have to face in a difference in perhaps degree, perhaps kind from the beyond HIPAA reports that this body talked about several years ago. This is all beyond HIPAA possibly unless it is a covered entity we are talking about. This is where I am going. What is first? How do we baby steps?

Andrea, I am hoping that when I read the article you gave us the link to, you have laid it all out for us. That is what I am hoping.

Andrea Matwyshyn: I tried. There will be a follow-up piece also of equal brevity. I think one of the baby steps that it would be very useful for us to consider effectuating would be to create a cross-agency taskforce, looking at the universal issues and identifying the regulatory core competencies of each agency and their mandate that already exist statutorily. Some of these are context-specific harms.

For example, the issue of employees being harmed when they leave one employer and go to another. That is something that the Department of Labor would be interested in. The issue of large-scale social, mental impact because of devices starting to cause questioning of the supremacy of sensory perception among our population. That is something that I think HHS and looking at these mental health questions and the way that they are impacted by devices in collaboration with say FTC or in particular CPSC is not at the table here.

CPSC is the agency that deals with safety of commercial devices that are non-medical. They are an agency that could be engaged to a greater degree and the FTC does not – I say this as an academic – does not perceive itself to be involved with safety at all. That is not how they perceive their space.

CPSC core safety concerns. They have not yet, as much as I would like to say, waded into questions of the way that software can kill people, for example, in IOT devices. But basically, each category of devices they regulate now has a software version that can hurt people. But there is not yet a response to the extent that I would encourage them to engage with these questions.

Same thing. Issues of machine learning. The way that the data is aggregated, created, validated, and what degree of integrity it possesses. Those are partially security questions. Those are also questions of how the things function and what ramifications they have on health and welfare of human beings who are using them.

The databases of aggregated merged information that are repurposed then for use by lenders and making decisions about whether to loan people money. These devices because they are potentially multi-function – nothing stops the aggregation of a body-embodied device feed from being merged with a social media feed from being merged with a credit report and then served up to a potential future employer, potential lender, a mortgage broker, criminal background check provider. There are lots of different directions where the well-being of humans can be impacted directly both in terms of physical safety and in terms of economic safety, mental safety, and health and just their life outcomes as members of our society because of the malleability, repurposing capabilities, and updating capabilities of these devices particularly as they get embedded or attached more permanently to human bodies.

We are already seeing the first cases of people getting kicked of insurance because of availability issues of internet access. CPAP machines, for example – they phone home to their insurers, and they are expensive. People rely on their insurance to cover them. But when people travel, for example, they cannot always get the CPAP machine on the hotel network because hotel networks are kind of glitchy sometimes and hard to get devices onto them or maybe the internet is down.

There have already been instances where insurers do not believe the insured that the device is in use every day but that there was just an interface problem with getting the device on the network. Here, you have the word of the technology and its lack of phoning home being taken over the sworn attestations of the insured whose well-being physically depends on the use of this machine and who cannot afford the machine otherwise. There are those kinds of scenarios already happening.

And looking at the patent activity happening in all of these spaces, it is very clear that there is an active investment ecosystem around all of these devices.

Melissa Goldstein: Fascinating. Thank you.

Others?

Linda Ricci: I think I would be remiss if I did not chime in a little bit about medical device authorities and where we have – what constitutes a medical device. I have seen a couple of questions in the chat about FDA, where their authority starts and stops.

In order to meet the definition of a medical device, you need to meet a 201(h). I am sure everyone is going to run out and read that right away because it is really a good read. But there is a specific definition of something that constitutes a medical device.

This was amended for the first time since 1975 with – I forget the actual – my apologies. That carved out from the definition of a device, certain software functions. This is where the multiple function language comes from with regards to a product that could have a medical device function and a non-medical device function.

FDA has issued guidance on our interpretation of this language for the software functions that were carved out of the definitions of the device and has issued guidance on expectations for devices that have multiple functions.

We do expect manufacturers for devices that have multiple functions to consider the risk associated with the non-device function on the device function. Looking more carefully at some of the information that Andrea has provided today, I can see how we will need to really think through that and what that looks like.

We have multiple digital health guidances and have been talking and put out a white paper, I guess is what I really want to say, about artificial intelligence and how it can be used.

Certainly, how you curate your data and how you train your network whether it is machine learning or expert system or whatever is going to impact what your ultimate results are. There can be a purposeful bias through the data that you curate. It could be a bias that you do not realize that is a result of how you curate your data. There could be a hacker that purposefully is manipulating your data so that there could be different results.

At the end of the day, whichever one of those cases it is becomes irrelevant to the end patient who is getting the wrong information – so making sure that as we are thinking through these advanced technologies and what their impact is to patients that we have appropriate controls in place to understand how this end patient can be impacted and to mitigate as much as we can for that.

Greg Garcia: I would go back to Andrea's recommendation about authorities' review, regulatory authorities across different health care issues. There are a lot of those and just coming from DHS and others, there have been so many attempts.

There is an organization – it is called something like the interagency cybersecurity regulators forum or council or something. It is like 20 or 30 regulatory agencies. The theory being that we are going to identify areas of overlap or regulatory conflict as it relates to cybersecurity for any given sector, industry sector.

But the fact of the matter politically is each regulatory agency has its statutory authorities. They answer to the Congress. Those kinds of legal and political and regulatory issues are so fraught. It would be a very heavy lift for just the Secretary of HHS as you are advising to make a recommendation to the White House to convene another group that would be focusing specifically on the range of health tech, med tech, whatever the terminology and how the different agencies can either help or hurt either the cybersecurity of health care or the products that feed into it through the supply chain. That is a big lift and it is complex.

I think the real focus needs to be on what are some of the tactical shorter-term things we can do to shore up our defenses and our preparedness.

Andrea Matwyshyn: I would like to push back on that a little bit. I think it is actually an easier lift than it might look at first brush because many of the agencies in question already have relationships and have working agreements in place. There are bilateral agreements that allow for issue-specific collaboration.

Some of this may not be an issue of creating a grand scale organization. I think it is more about decision makers, key decision makers and agencies creating targeted teams that are working together on identifying their shared authority and their individual authority on these issues.

For example, FTC and FDA have been working together well for a long time. That is one set of teammates that are used to that collaboration, bringing in CPSC, for example, creating a triumvirate, looking at these issues. Suddenly we have an octopus with tentacles that are going out in more directions. Then you bring in another agency and maybe we do this from a grassroots way or you just create bilateral relationships. But I think HHS taking an interest in this and building out some of their own targeted relationships would go a long way.

For example, in particular, the Department of Labor has expressed interest in security recently and in building out workforce. I think the issues of employees that the Department of Labor looks at and the health and welfare issues that are within HHS' purview, that is a really nice match of issues and so a bilateral relationship, looking at these internets of bodies' devices in that context could go a long way, I think.

Greg Garcia: We need to keep trying but the 25 years I have been working on it has not been very effective as an interagency process. It is too much. It is too complex. I think we need to focus on the tactical efforts.

HHS has a lot of work just to coordinate internally within HHS. You have ASPR. You have OCR. You have ONC. You have CMS. You have CDC. All of these operational divisions touch on different aspects, different statutory authorities related to health care and by extension, health care cybersecurity. None of that is really effectively coordinated. I will not say – they are counterproductive to each other. But they all have different statutory authorities.

I take your point. It is a noble goal and there have been any number of attempts to do that. I think there are success stories at a bilateral level or trilateral level. But it is a much bigger problem than that. The federal enterprise is a big, messy machine.

Jacki Monson: Thank you.

Maya.

Maya Bernstein: Tammy has her hand up. I always defer to members first.

Tammy Banks: Maya, I did not mean to jump in front of you here. But I just want to say I really appreciate all of you being here. This has actually been very thought provoking, somewhat concerning in some pieces. Referring the maturity curve of cybersecurity to quality kind of raises concern. However, it does show some successful pathways of possibly raising the priority across the health care industry because we do know that privacy and security is not necessarily the first thought when standards are developed, which really should be the ultimate first steppingstone.

But the question for you guys that I keep pondering on and I do not have an answer is when we look at it from a health care standard perspective, we know that data fluidity has been between the payer and provider and we want to make sure to move that information as safely and securely as possible. But now that pathway has expanded into the patient that the patient is now part of the process and will be continuing to be more part of the process. We know that patients are the ones who own their data. They are uploading the information within these different systems. They are using their own phones, their own computers.

What kind of pathway do you feel or what should we be thinking about to ensure the protection of the patient's data when it comes from their residence especially as we move to hospital at home and all these other important product lines to try and provide the care where the patients need it? We know the patient is not a protected entity under HIPAA. What kind of thought processes have been going on around that aspect?

Linda Ricci: From a medical device perspective when patients start to use their own device as part of the medical device to collect information, it is really important that we think about this in terms of zero trust. You create zero trust architectures. And then this is where threat modeling is really important and thinking about what is it that you are trying to protect. Without going through the process of a threat model, I think it can be really challenging to get to that answer.

As a patient, putting on my patient hat, not my regulator hat, I want to have access to my data. It is my data. I need to have access to that. There are secure ways to do that. Is it an easy problem? It does not have to be a hard problem. There are technologies that you can use in the design of the system that allows for zero trust. You can protect the data and still allow access for the patients and allow that data and that information to flow into medical records. For medical devices, we need to be able to use this data to control something. We have to be able to crate the zero-trust architecture around this so that it can be safe and secure.

Jacki Monson: Maya.

Maya Bernstein: There are no other members. This panel turnout. Thank you so much, everyone, for coming. When I planned this, I had no idea this would be – I knew it was going to be cool, but I did not know it was going to be this cool.

Let me say I have a habit of thinking about cyber infrastructure, the kind of work that our infrastructure protection team, Greg, Reuven, and others do as a kind of a macro-level thing. I think of it as focusing on hospital systems and big ticket. I want to know if I am thinking about that wrong. The kinds of stuff that Andrea is bringing up, the kinds of things that Linda is talking about at the more micro-local level. Is our agency for preparedness and response, DHS, the infrastructure coordinating committee thinking about infrastructure on that level if not for today? Is there a plan for incorporating the sort of micro-level of the infrastructure when patients are going to become part of that network as Tammy pointed out? Is that in the works or is it really that we are focused on macro and how can we – if that is not in the works – I guess we have been talking about what we should be doing moving ahead, who should be regulating, or how we should be managing this. But shouldn’t it be part of our infrastructure protection, seeing the way that the future is going?

Reuven Pasternak: Maya, I would be interested to hear what my colleagues say about that. But I agree with you. That, to me, is a very scary part of the direction when I mentioned the fragmentation of the health care system because people are increasingly taking small bits of their health care and dealing directly with parties and not aware of some of these issues. They take out their cell phone and they pay for their service. They transmit information. That definitely is a frontier of maturing the public awareness and information. What can be done technically about it? There are others who know more about this than I. I am sure that is going to be part of it. Putting out there as a concern for the frontline interface between the patient and the system is definitely something of major concern.

Maya Bernstein: Can I modify my question a little bit, given your response. Thinking about educating patients or consumers, given what we are currently doing, where we have that box of 69 pages of text in a frame that no one is ever reading and just clicking I accept. That is public education apparently, but that is not effective or working in any way. I have very little confidence in that truthfully.

I am also thinking – someone brought to my attention when we were thinking about some of these issues that there is a national security angle to this, which is that you do not know if the app that you are using to download onto your personal device, easy health one, two, three, is provided to you by the Chinese government. This was a serious suggestion that came to us from a detailee that was here from the FBI.

In terms of security writ large, are we thinking about what is coming as we are pushing stuff more to the local level or the patient level? I have to say that I have very little confidence that patient education is really the answer.

Greg Garcia: We are thinking about that. I think I mentioned to you in my initial comments in the slide deck that I think one of the best pieces of work in terms of looking at the national cybersecurity threat profile is really an aggregation of what is happening on the ground whether it was connected medical devices or wearable medical devices, medical devices in the home, or all the other aspects, workforce problems.

The Health Care Industry Cybersecurity Task Force has pretty much served as our strategic guide. In cooperation with the White House and HHS and CISA, we are going to be embarking over the next year on updating that and really looking at – I think to your point, Maya. What does the health care system of the future look like? How much of health care and health care data is going to be transferred directly to the patient? A lot of home health care is going to be happening. How does that affect our enterprise health care? How does it affect personal health care and data, data protection? How do we prepare for that from patient education all the way up to national standards for cybersecurity in the health care industry?

We are going to be undertaking that strategic review as to how we address that continuum from the patient all the way up the stack to national-level health care systems, pharmaceutical, and medical device manufacturers. That does not really answer your question.

Participant: It kind of does. You are thinking about it, which is what I wanted to know. We are not there yet.

Greg Garcia: CISA has this – and part of it is just – I started 20 years ago in cybersecurity almost full time. You could not get anyone to talk about cybersecurity. And now, look at the nightly news. Half of the television commercials are about your iPhone is more secure than the next guy’s phone. Our connectivity is more secure. Think about your cybersecurity. It is like everywhere now. But it still has not permeated the national culture, the national psyche.

CISA has not a bad slogan. If you see something, say something. What is our slogan. In the Sector Coordinating Council, we tend to say cybersecurity safety requires patient safety or patient safety requires cyber safety, either way you look at it. Getting that sort of into the day-to-day thinking as a habit is a tremendous cultural undertaking as well as a technical one. We really do have to deal with that at a national strategic level, regulatory level as well as down to the day-to-day users.

One of the things we are working on in – we have a workforce development task group in the cybersecurity working group. We just received funding from a couple of our member organizations to produce a ten-part video series called Cybersecurity for the Clinician, not cybersecurity for the geek, the clinician. That is, if you are a nurse, a surgeon, a GP, you are touching data or you are a medical student. You are touching data. You are touching patients. You are touching medical devices and in all of those situations, you, as a clinician, are a vector for a cyber attack because of both vulnerabilities and threats and your own complacency or lack of training. There are simple things everybody needs to understand that they have certain responsibilities for. It is not just the IT guy’s problem. This is what we are trying to get across.

We are hoping that this series of videos, five to seven minutes each, because that is the attention span you have gotten with the surgeon, who has to get back into the operating room. But we are hoping that this will get CME credits, get certified for continuing medical education credits. We are going to have a number of medical schools kick the tires and circulate these videos to their medical students. Perhaps one day some of them will become required as part of your graduation requirements.

And just bringing awareness down to those who are on the frontlines every day. You have to keep banging the drum. It is truth by repetition. And at the same time, we are doing that. We have to work with the government to figure out what are those incentives that are going to drive investment and execution of the basic cyber hygiene that is going to protect health care systems and their patients.

Linda Ricci: And FDA has worked with patients directly. The CDRH has a patient advisory committee. It is called PEAC, P-E-A-C. There was a PEAC Advisory Committee on cybersecurity so that we could – when we issue safety communications around cybersecurity, we can do that in such a way that patients understand what the impacts are about.

We have also used that opportunity to think about what patients want to know about their device and cybersecurity. And we have created a video targeted towards patients, describing cybersecurity and what they can do. We can create these resources. But, again, getting people to view them and watch them. We need to incentivize that in some way. We need to make sure that this is part of our continual discussion.

I used to – any time I did a conference presentation, I would say I have to say cybersecurity at least five times during this presentation or I am going to get fired. It is just that kind of continuing to bring it to the attention and to make it more approachable.

We cannot say that cybersecurity is this great big, hairy thing that you have to have a PhD to understand. A, it is not true. B, it has to be approachable so people feel like they can be empowered to do something about it.

Greg Garcia: It is generational. We have children at age 3 have iPhones and iPads in their hands. They are coding. Old guys like me have learned it slowly over the years. But this is native to them. I hope – I have some confidence that over time not only will the users be more sophisticated, but the user interface will become easier where there is the usability of cybersecurity is less of an inconvenience or some kind of cipher we cannot understand. It should be as easy as locking your doors at night. I think that is where the technology and human psychology will come together.

Jacki Monson: We are at time. Denise, I see you have a question, but we are unfortunately out of time. I just want to thank all four of you for all of your time with us this afternoon, for your dedication to presentations and all you are doing for cybersecurity in health care. Hopefully, we are all in it together and can solve it before 25 years from now, which is how long it took for cyber hygiene hands. Anyway, thank you so much.

We are going to now move to public comment, Rebecca.

Public Comment

Rebecca Hines: Can we have the public comment slide instructions?

Margaret Skurka: Are we not going to have my report on ICD-11?

Rebecca Hines: That is coming up after public comment.

Thank you very much. Most of you are on Zoom and Zoom audio and you are welcome to raise your hand to have your audio unmuted or you can use the Q&A to request an open audio line. I do not know if we have anyone on the phone. We have one person on the phone and a member on the phone. You can press *9 to request that your phone be unmuted. You can send an email to NCVHS, which I do not see anyone has.

We have one question here from Ogi Quan (ph.). Ogi, would you like – I will read this into the record and then members do not need to respond today but just to get it into – for their information. Your question or your comment is I did not see any mention of payer portal direct data entry regulatory recommendations on today's presentation materials.

If this correct, could you explain why that is and whether the committee no longer considers this a priority despite feedback from the 2021 listening session and our Full Committee meeting in January? From our perspective, payer portals can be administratively burdensome for providers to navigate and often include among other things, highly restrictive terms of use and prohibitions on automation. Thank you very much.

The members do not have to respond, but we can certainly take into account your inquiry. Thank you.

Any other comment for the record? Again, the instructions are on the screen. Just for the record, there was another comment this morning in the Q&A, pertaining to Standard Subcommittee recommendation number two on updating systems. Is there an end date on moving towards a new version? I wanted to get that in the record from Lisa McKeen.

We have an attendee. Mike Denison. Can you open his line, please. Mike, can you state the organization you are with? We are not able to hear you. Are you speaking, Mike?

Mike Denison: This is Mike Denison. I am providing comments as an individual. I just wanted to let the Subcommittee know that I have sent my comments via email.

Rebecca Hines: Thank you, Mike. If I receive them in the next 30 seconds, I can read them into the record; otherwise, we can attach to the meeting summary.

Mike Denison: There are several comments. It may be best to attach them.

Rebecca Hines: Okay. Thank you.

I think that is it for now. There will be another public comment period tomorrow afternoon. We will be returning to the proposed four recommendations letter tomorrow afternoon where it says follow up on Day 1 on the agenda. I believe that is after the public comment at 3:30 tomorrow.

Jackie, I think the plan is to go back to the update from Standards now.

Standards Updates

Jacki Monson: It is. I want to turn it back to Rich and Denise to provide an update on Standards and Margaret to provide her on update on ICD-11.

Rebecca Hines: Rich, you are still muted on the phone. *6 yourself and hopefully you can get a live audio. We have the first slide, the cover slide up since we know you cannot see the screen. We still cannot hear Rich's audio, Sabira. Any suggestions?

Participant: It looks like he unmuted now.

Rebecca Hines: Okay, Rich. Thank you. We have the title slide up.

Rich Landen: Thank you. The IT gods are not cooperating out here in New Mexico.

Overview of what besides the Convergence 2.0 project that we discussed this morning that are on the plate for work by the Subcommittee on Standards. First, I would like to talk a little bit about the requests to review HIPAA Transactions and Operating Rules. We at NCVHS have received a request from X12 to look into, make recommendations on updates to the three HIPAA claim transactions, the X12 837 Professional, Institutional, and Dental Claim Implementation Guides, as well as the 835 Payment/Remittance Advice Implementation Guide. X12 is proposing from version 5010 to version 8020. The Subcommittee will be meeting with X12 soon for an overview and then in the next quarter, we will schedule a public listening session, probably one day. And we will get industry input on that.

Separately, CAQH CORE, which is the designated operating rules authoring entity, has submitted a letter to NCVHS proposing updates to three of its existing rules that have been adopted by CMS under HIPAA. First, is the Connectivity Rule. Second is the Infrastructure Rule. And third is Eligibility and Benefits Data Content Rule. In addition to those three updates, CORE is proposing adoption of two new rules. One is the Attachments Rule and the other is the Eligibility and Benefits Single Patient Attribution Data Content Rule. I will talk a little bit more about those in a minute.

The other major item the Subcommittee has on its plate is the ICD-11. We, at NCVHS, have sent two letters of recommendations to HHS, requesting research into the goodness of FIT for ICD-11 for US health care morbidity purposes, including determination of the necessity or lack of necessity to continue a US-specific clinical modification.

Then we also talked about some of the mortality. Margaret Skurka will then walk us through the status of the US and internationally of ICD-11.

X12 requests to review HIPAA transactions. As I mentioned, we have the request for the claims and the payment remittance advice. All four of these implementation guides, all four of these adopted transactions are highly utilized by the industry. The claims are upwards of 90 percent for institutional and professional, 84 percent for dental. And the Payment/Remittance Advice is 76 percent for medical and 84 percent for dental. That is kind of reflective of what I had talked about this morning when I was talking about the installed base and that the existing transaction versions that are working need to be protected so we are not talking rip and replace here.

The request from X12 is to move from Version 5010 to Version 8020. 5010 was validated by X12 back in 2003 and it was adopted under HIPAA by CMS by final rule in 2009 with an implementation by the industry in 2012. It is a little bit long in the tooth. But as the usage statistics show, it is still a good transaction.

8020 was balloted by X12 in 2020. It is much more up to date although it is still two years old and the implementation rule promulgation process if it goes through the regular notice of proposed rulemaking, public comment, and then final rule making and an implementation window. We are still looking at least two years for the final rule and another year or two for the implementation period.

If we move to slide 4, the number of enhancements in each of those implementation guides is shown here for the professional and institutional claims. The number of enhancements or changes to the implementation guide exceed 1000 that is given the long-time span between the last update and this update. That is not unexpected. For the dental claim, the number of enhancements is 333 and for the remittance payment/advice, it is 259.

The committee work plan is this month. The Subcommittee will get an overview presentation from X12 that will help us scope the project and plan what we need to do to organize and conduct an effective listening session for public comment. We are assuming based on past experience that we will be doing a one-day listening session some time in the third quarter. Before that happens, we will publish a Federal Register Notice about the meeting, giving the details of the date and how to access it along with a request for whatever comments the industry has. It remains to be discussed by the Subcommittee after hearing the overview from X12, whether or not we will come up with a specific list of questions that we are interested in hearing from the industry regarding the updates to the four transactions.

If all goes to plan and we are reasonably confident that the calendar works out, we will bring back draft recommendations to the full NCVHS action at our next meeting, which would be November or December some time.

Shifting over to CAQH CORE. As I mention, three updates and two new rules. And then slide 7, the work plan for us is similar to X12. We will get an overview presentation by CORE in August. We will conduct what we believe is a one-day listening session. The X12 listening session and the CAQH CORE Operating Rules listening session will probably be back-to-back days, again, with Federal Register Notice and request for comments.

Just like the X12 recommendations, the CORE Operating Rules and Recommendations we would envision bringing to the Full Committee for discussion at the November/December meeting.

Let me pause here and ask my Co-Chair Denise Love if she has any additional comments for this or anything else on the Subcommittee’s plate.

Denise Love: No. You covered it. Thank you.

Rich Landen: That is the Standards world. Shifting now to ICD-11. I will go through the next two slides and then I will turn it over to Margaret Skurka for the status around the world.

ICD-11 was adopted by the World Health Organization at the end of May of 2019. WHO or the World Health Assembly set an effective beginning date for January 1, 2022. ICD-11 has three specific components. First is mortality, death reporting, cause of death reporting. Second is morbidity --

Rebecca Hines: Rich, hold on. We were looking at the CAQH CORE slide. We are now on the ICD-11 slides.

Rich Landen: As I mentioned, adopted by the World Health Organization in May 2019 with an effective date scheduled for January 1, 2022. Three components to ICD-11. Mortality, cause of death, death reporting, morbidity for US health and care and public health, which is more statistical and population health information, and then finally, morbidity for US health care billing and payment. The third is kind of the aspect that we are focusing on as a Subcommittee.

The mortality reporting is a condition of membership and the World Health Organization. Effectively, we are deeming that a treaty obligation and there is not a regulatory process to go through to administer that. We are effectively monitoring that and again doing the research to ensure that ICD-11 is developed by the World Health Organization, which included representation from the US, is appropriate for the uses here in the US.

But specifically, down to the morbidity for US health care billing and payment, NCVHS is on record. We have sent a couple of letters to HHS asking or recommending, to conduct research into determining how well or how poorly ICD-11 would meet US needs and to develop a communications plan to avoid – to inform the end users, the stakeholders about the ICD-11 and determination of value of ICD-11 over ICD-10.

And then also top of our mind is the several postponements in the transition between ICD-9 and ICD-10. We want to make sure that we capture the lessons learned from that and we avoid the mistakes we make and then hopefully can shepherd the process through a much more orderly transition than we saw from between 9 and 10.

Shifting to slide number nine, HHS acknowledged the NCVHS recommendations. There has been some research done within the National Institutes of Health, National Library of Medicine. And to that end, we had a presentation back in March of 2021 by Dr. Kin-Wah Fung. We, as the Committee, received some additional insight from Robert Anderson in March of 2022.

Nonetheless, the studies that we recommended have not yet been done. We had a very recent conversation with CMS, the Office of Burden Reduction and Health Informatics. Pardon the transposition of the letters and the acronym there. But OBHRI and the Division of National Standards is proposing a budget request in their fiscal year 2023 budget, seeking monies to support the research that we recommended.

The Standards Subcommittee is continuing to collaborate with OBRHI, the other agencies, and the private sector around research design and industry expert convenings such that we will be able to assist CMS in its approach to study for the implementation of ICD-11.

The subcommittee objectives are unchanged. Vetting ICD-11, including the potential clinical modification, doing research and communications plan, and as I mentioned, avoiding the repeat of the ICD-10 transition dysfunction. Those are the highlights of where we are process wise.

I will turn it over to Margaret Skurka, who can talk much more knowledgeably about the prognosis here in this country and has some specific information about ICD-11 status in other countries.

Margaret Skurka: Thank you. I just wanted to add that we will not have the debacle that we had from 2009 to 2015 because that is what happened with the last addition with 10. As I traveled, I was doing some WHO work at the time and I just – people looked at me incredulously and said you guys are still not there. Well, we were not. It was a very long process.

We know now that 30 countries – they are small ones. They are not the big three, which is Australia, Canada, and us, have already transitioned. We need to move this along certainly in our country. It will get better and one of the reasons it will get better is at this time is because we are not dealing with the procedure system because we were doing both last time. So PCS and that was brand new. That was a whole different concept. That slowed us down a little bit. Now, we are just focusing on the diagnosis ide.

I heard from Rich over the weekend, and I reached out over the weekend to my counterpart in health information management in Canada and Australia. This is current news from them as of this week. In Canada, work is underway to assess transitioning ICD-11 with consideration for timelines and implementation. They do not currently have set a timeframe as to when it will be implemented but they are starting their work. I was told they are assessing the level of specificity that is able to be captured with this system and whether a Canadian version of I-11 is required.

Let me just say from the outset there that the WHO is discouraging as best they can for any country to do a modification. They say if you identify something that is not in it, tell us now and we will add it. They really do not want – this should be one coding system that is workable for the entire world.

Australia. I heard back from them right away. They have not made any formal decisions yet to move to ICD-11 as of Monday. They are hoping to not do a national modification also. They are considering it and it is just a consideration. We are all trying to cooperate here with WHO so there is one system for the world.

They told me to answer to whether they will do a modification and will inform the decision to implement and impact the target data for implementation. It certainly can be sooner if they are not going to make any changes to it. And they already have in place an ICD-11 task force to consider the issues of a national modification and other issues.

They are going along, and we need to do the same here in this country and I think get a task force together and start to study the issue. If I can be helpful in helping move that along, I am all in. Thank you.

Rebecca Hines: Can we have the next slide?

Discussion

Rich Landen: I think at this point, I will invite any members of the Subcommittee on Standards if they have comments about what is on our plate. After that then we will go see if any of the NCVHS members have questions for the Subcommittee.

Rebecca Hines: Vickie’s hand is up, Rich.

Vickie Mays: Thanks. In terms of the meeting that we had about ICD-11, I cannot remember when it was now, year and a half ago, we made several recommendations. Did we get back any response to those?

Rebecca Hines: Yes.

Rich Landen: Yes, what we got, Vickie, is pretty much just a letter of acknowledge, a letter of receipt. But I am happy to report that the meeting between the Standards Subcommittee co-chairs and OBRHI, OBRHI did indicate that it is taking on some responsibility for looking into research for ICD-11 and they told us that they are looking for budget monies for next fiscal year to initiate some research. Their plans are not definite. The budget monies obviously are not yet in hand. But there is a commitment that we will work together and as OBRHI pursues its goals, we will – the NCVHS and the Subcommittee on Standards, will work with them so that we can both bring our strengths to bear. We are thinking in terms of some – maybe the NCVHS sponsoring some convenings of experts or industry panels, and generally working through the process side by side.

Denise Love: Vickie, may I add, we also have those research questions that were promulgated from that day and a half long workshop. They were very good questions. I think Mary Green, Dr. Green acknowledged. They have those questions.

Vickie Mays: I am going to assume then that we are going to track, keeping this kind of in a time – this will be done in a timely fashion, because that was the big push that came out of that meeting is it is just like what Margaret was saying, we can't wait forever. And this time, we need to do these sooner rather than later because they significantly impact the mortality data stuff at NCHS and the Social Security Administration, and a couple of other places. I am assuming that you all are tracking the timeliness of this.

Denise Love: The mortality is moving on its trajectory because it was required. It will be on its own path. We will be interested in how that path goes because – inform morbidity when morbidity comes online. But the morbidity is really the focus of the research questions and I think what we will be watching closely.

Margaret Skurka: And remember, it is online. The whole system is online. It is free. There is no more books. So it will help things go quick.

Denise Love: Well, quick, we hope.

Margaret Skurka: Go out on a Friday night with a glass of wine or something and just knock around. Put in your favorite diagnosis. You too will be coded.

Denise Love. High hopes.

Rich Landen: Are there any other questions?

Denise Love: Yes, Rich. Are biweekly meetings enough?

Jacki Monson: I do not see any other questions. Is that it for your update, Rich and Denise?

Rich Landen: That is all.

Jacki Monson: Is there any other business we have to address today, Rebecca?

Rebecca Hines: No. At this time, unless there is other discussion, we did not really get any public comment to discuss. It is up to all whether there is anything else you want to discuss today. I see a hand up from Maya Bernstein.

Maya Bernstein: I just wanted to know if you wanted to go over the schedule for tomorrow since it has changed a little bit from what people may have reviewed before just before we adjourn.

Rebecca Hines: That is a great idea. We can actually update the website this afternoon, as well. We are going to start at 11:30 tomorrow. And after roll call and agenda review as the agenda says, we will have the update on the SOGI and SDOH Workgroup. And then at noon, we are going to the panel on Legislative Developments in Data Privacy. We expect that to actually go to 1:30. Just note that we expect that to be a 90-minute panel because just as with today's panel on cybersecurity, we have a wonderful set of experts, and we anticipate we will need the full 90 minutes.

We will have a 30-minute break. And then Tribal Epidemiology Centers Panel. That is expected to be 90 minutes as noted on the agenda. We will have public comment. And then at 3:45, we are going to need to go back to the Standards letter. I would imagine we might need 45 minutes for that. We can add 15 minutes to the agenda to discuss the work plan or not. That is really your call of the members.

But I would imagine everyone should try to be available until 5 p.m. Eastern in case the Standards letter takes a little longer. Hopefully not. We do have a challenge with one of the members internet just went out. Rich's internet went out. But we are going to hope that that comes back on in the next few hours and we can have a letter out this evening for everyone to review.

Anything else, Maya, that you think we should touch base on or Jacki?

Jacki Monson: No, I think we are good to adjourn for the day.

Maya Bernstein: The only thing I would add is I was very pleased that during the meeting today, we confirmed a second tribal epidemiology center representative, the CEO of the Great Plains group is going to join us. I think that is going to be really interesting. I am hoping that you will raise some of the questions you had today of the Cybersecurity Panel with the people who are going to talk to us about legislative updates, states, federal, and international tomorrow.

Jacki Monson: I think it is going to be another great day of lots of good content. Thanks, everybody, for your time and attention today. We will see you all tomorrow at 11:30 a.m. Please do look for the letter, a draft of it tonight so we can try to get through approvals tomorrow. Thank you.

(Whereupon the meeting was adjourned at 4:30 p.m.)