Department of Health and Human Services
NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS
July 20-21, 2022
Virtual Meeting

MEETING SUMMARY

Note: *For details on this meeting, please refer to the transcript and slides posted here:* https://ncvhs.hhs.gov/meetings/full-committee-meeting-11/

The National Committee on Vital and Health Statistics (NCVHS) was convened virtually on July 20-21, 2022. The meeting was open to the public. Present:

Committee Members
Jacki Monson, JD, Chair, Sutter Health
Tammy Banks, MBA, FACMPE
James Ferguson, Kaiser Permanente
Melissa Goldstein, JD, GWU
Richard Landen, MPH, MBA
Denise Love, MBA
Vickie Mays, PhD, MSPH, UCLA
Margaret Skurka, RHIA, CCS, FAHIMA, IU
Debra Strickland, MS, Conduent
Valerie Watzlaf, PhD, MPH, RHIA, FAHIMA, UPitt
Wu Xu, PhD, University of Utah

Executive and Lead Staff
Sharon Arnold, PhD, ASPE, Exec. Staff Director
Rebecca Hines, MHS, NCHS, Exec. Secretary

NCVHS Staff
Maya Bernstein, JD, ASPE/OSDP
Lorraine Doo, MPH, CMS
Jim Craver, NCHS
Marietta Squire, NCHS

Invited Speakers
Jerilyn LeBeau Church, MSW, Great Plains Tribal Leaders' Health Board
Kristin Cohen, JD, Federal Trade Commission
Abigail Echo-Hawk, MA, Urban Indian Health Institute
Kristin Ekelund, MSSA, Government Accountability Office
Greg Garcia, Health Sector Coordinating Council
Stacey Gray, JD, Future of Privacy Forum
Kirk Greenway, PhD, IHS
Andrea Matwyshyn, JD, PhD, Penn State
Heather McLane, MBA, IHS
L. Reuven Pasternak, MD, MPH, MBA, Department of Homeland Security
Linda Ricci, MME, MPH, FDA
Lauren Riplinger, JD, AHIMA
Tricia Roy, MPA, Government Accountability Office
Cobun Zweifel-Keegan, JD, CIPP/US, CIPM, IAPP

Others
Susan Jenkins, PhD, ASPE
Rachel Seeger, MA, MPA, OCR
Grace Singson, PharmD, MS, ASPE
Ryan Mintz, ASPE

In addition to those individuals who presented virtually during the meeting (listed above), 95 people on Day 1 and 79 people on Day 2 followed the meeting online.

ACTIONS

1. The Committee approved the Subcommittee on Standards letter and recommendations (with additional non-substantive refinements related to citations and formatting to be performed by the Subcommittee) to the HHS Secretary on modernizing the adoption of HIPAA transaction standards.

The final version of the letter and attachments will be posted on the NCVHS website.

—DAY ONE—

Call to Order and Roll Call—Rebecca Hines, Executive Secretary and Designated Federal Officer

Ms. Hines invited National Committee on Vital and Health Statistics (NCVHS) members and speakers to introduce themselves and state any conflicts of interest pertaining to the meeting. No attendees stated a conflict of interest. Ms. Hines stated that the remaining 2022 NCVHS meetings will be held virtually, and NCVHS will schedule the next Full Committee meeting in late November or early December. Members and participants can view updates on upcoming meetings on the NCVHS website.

Welcome Remarks and Agenda Review—Jacki Monson, Chair

Ms. Monson welcomed NCVHS Committee members and invited speakers to the meeting and reviewed the meeting agenda.

Update from the Office of the Assistant Secretary for Planning and Evaluation (ASPE)—Sharon Arnold, Executive Staff Director

Update on Return to Office

Although ASPE leadership has worked in person at the agency's headquarters in Washington, D.C. throughout the COVID-19 pandemic, other staff continue to work remotely—partially because the initial return-to-office date in early 2022 was delayed due to the Omicron variant. ASPE has continued to invest in technology and electronic infrastructure upgrades to support hybrid and remote work capabilities. The Department of Health and Human Services (HHS) recently ranked second highest in engagement satisfaction on the Federal Employee Viewpoint Survey, and both ASPE and HHS as a whole strive to keep employees engaged and connected. ASPE will continue to follow Centers for Disease Control and Prevention (CDC) guidance on COVID-19 precautions when considering plans to return to the office.

ASPE continues to respond to major physical and mental health concerns linked to recent events, including rising COVID-19 case numbers, multiple mass shootings, and the U.S. Supreme Court decision in Dobbs v. Jackson Women's Health Organization. In May and July, multiple HHS units responded to communities impacted by mass shootings (e.g., Uvalde, TX, and Highland Park, IL), including providing residents with access to crisis counselors and CDC guidance for communities on preventing gun violence.

Sexual and Reproductive Health Access

In anticipation of the Supreme Court's decision in Dobbs v. Jackson Women's Health Organization, HHS Secretary Xavier Becerra established the Interagency Task Force on Reproductive Healthcare Access in January 2022 to facilitate approaches for protecting access to sexual and reproductive health care services. Following the Supreme Court's decision, Secretary Becerra announced HHS's action plan for maintaining reproductive health access, which focuses on six key priorities:

1. Increasing access to medication linked to reproductive and sexual health
2. Protecting patients and health care providers from discrimination
3. Ensuring privacy for patients and health care providers
4. Protecting access to emergency abortion care
5. Ensuring health care providers have access to family planning training and resources
6. Strengthening family planning care, including access to emergency contraceptives

Since the announcement of this action plan, HHS has undertaken multiple initiatives:

- HHS launched a website describing reproductive rights to enhance public awareness.
- Secretary Becerra and Secretary of Labor Marty Walsh met with major health insurers and encouraged them to provide no-cost coverage for contraceptive services as required by the Patient Protection and Affordable Care Act.
- The Office for Civil Rights (OCR) published guidance for patients and health care providers on the degree to which the Health Insurance Portability and Accountability Act (HIPAA) protects privacy of patients seeking contraception and other reproductive health care. This guidance includes health information stored in mobile apps and devices.
- The Office of Population Affairs announced $3 million in additional funding for Title X family planning and expanding access to reproductive health care.
- HHS has issued guidance clarifying that emergency health services include emergency contraceptive and abortion care. This guidance reiterated that pharmacies are required to provide access to contraceptive medications.

Continuing Response to COVID-19 Pandemic

On July 15, 2022, Secretary Becerra renewed the state of emergency declaration for the COVID-19 pandemic, and CDC continues to track and disseminate key pandemic data, such as hospitalization, death, and vaccination rates. In March, CDC transitioned from using community transmission metrics to track COVID-19 prevalence to community-level metrics, which assess the impact of COVID-19 infection on different communities, including transmission, hospitalizations, and impacts on community health care systems. CDC now recommends using community-level metrics to inform public health responses to the COVID-19 pandemic.

The BA.5 Omicron SARS-CoV-2 variant is currently predominant throughout the country. Current COVID-19 case rates are underreported due to increased usage of at-home testing; thus, CDC continues to support the National Wastewater Surveillance System to assess SARS-CoV-2 prevalence in communities that may not be captured through traditional reporting channels. Approximately 50 percent of monitoring sites are reporting increasing prevalence of SARS-CoV-2 levels, with many sites showing levels matching the Omicron spike in December 2021.

On March 29, 2022, CDC recommended that individuals aged 50 and older and immunocompromised individuals obtain a second COVID-19 booster shot. On June 17, 2022, the Food and Drug Administration (FDA) expanded the Emergency Use Authorization (EUA) for the Pfizer and Moderna COVID-19 vaccines to children aged 6 months and older. In July 2022, FDA revised the EUA for Paxlovid to enable pharmacies to prescribe Paxlovid to eligible patients with SARS-CoV-2. FDA also provided an EUA for the protein-based Novavax COVID-19 vaccine, which is an alternative to mRNA-based vaccines.

ASPE has published multiple reports in 2022 on the COVID-19 pandemic, including two reports on vaccine hesitancy among parents. ASPE also published a scoping report examining impacts of social determinants

of health (SDOH) on COVID-19 infection and hospitalization risk, as well as the reliability of COVID-19 data on major federal data platforms.

Other Public Health Needs

HHS continues to monitor other public health concerns. For example, worldwide measles cases increased by 79 percent in the first 2 months of 2022, compared to the same period in 2021. A recent UNICEF report identified how pandemic-related disruptions and the diversion of resources toward COVID-19 vaccinations have increased inequities in access to vaccines for measles and other preventable diseases. As communities relax social distancing, masking, and other public health practices instituted during the COVID-19 pandemic, the risk of large-scale measles outbreaks increases. Furthermore, international conflicts and large-scale population displacements in countries such as Ukraine, Somalia, and Afghanistan impact the ability to distribute and provide routine vaccinations, further increasing the risk of outbreaks of vaccine-preventable diseases.

President Joe Biden recently announced an initiative to establish the Advanced Research Projects Agency for Health (ARPA-H). ARPA-H will be an independent agency within HHS that funds research and development for therapeutics, technologies, and other products to transform health care and public health responses.

The Biden-Harris administration established the HHS Office of Environmental Justice (OEJ) on May 31, 2022. OEJ represents HHS in the Justice40 Initiative, which directs that at least 40 percent of overall benefits of investments in climate change, sustainable energy, and affordable housing programs flow to communities that are marginalized and disproportionately affected by pollution and climate change.

HHS is also involved in government-wide efforts to address mental health crises, including addressing burnout, depression, and suicidal ideation among physicians and other health care providers. In July 2022, HHS and the Federal Communications Commission launched 988 as a national suicide prevention and 24/7 crisis care hotline to replace the previous 10-digit hotline number. 988 also links with the Veterans Crisis Line to provide additional assistance and outreach to current and former service members who require crisis mental health services.

In February 2022, CDC released updated clinical practice guidelines for prescribing opioids for chronic pain based on updated research. In fiscal year (FY) 2023, HHS has allocated $21 billion to evidence-based treatments for opioid use disorders. This allocation includes $10 million in grant funding to increase access to substance use disorder treatments in rural areas, $1.5 billion to support state opioid crisis programs, $55 million for Tribal programs, and $44 million for mental health and substance use disorder treatment services for those living with HIV.

HHS FY2022–2026 Strategic Plan

In 2022, HHS released its 2022–2026 strategic plan, which has the following five strategic objectives:

1. Protect and strengthen equitable access to high-quality and affordable health care
2. Safeguard and improve national and global health conditions and outcomes
3. Strengthen social well-being, equity, and economic resilience
4. Restore trust and accelerate advancements in science and research
5. Advance strategic management to build trust, transparency, and accountability

Discussion

988 Suicide Prevention and Crisis Care Hotline

Dr. Mays asked whether the Substance Abuse and Mental Health Services Administration (SAMHSA), which manages 988, is collecting data on 988 users to determine if particular populations or demographic groups encounter obstacles in accessing suicide prevention services. Dr. Arnold will determine whether SAMHSA is collecting these data and will follow up with Dr. Mays with her findings.

Mental Health Questions in NCHS Surveys

NCHS previously collected mental health data through its surveys, but the responsibility of tracking this information was later transferred to SAMHSA. This shift has caused difficulties in linking mental health data with other health and wellness outcomes. Dr. Mays asked whether NCHS will include mental health questions in its surveys to address this issue. Ms. Bernstein replied that NCHS is assessing whether to include mental health questions, reviewing policies to ensure compliance with HIPAA and substance use disorder treatment confidentiality rules, and coordinating next steps with SAMHSA. Mr. Landen noted that the Subcommittee on Standards efforts to update HIPAA regulations as part of its Convergence 2.0 project include improvements in data flow to improve data linkages across agencies.

Improvements to Collection of Racial and Ethnic Data in COVID-19 Community-Level Metrics

CDC's new community-level metrics for SARS-CoV-2 cases capture race/ethnicity data. Dr. Mays asked whether CDC is encouraging states and municipalities to capture more comprehensive and accurate data on race and ethnicity. Dr. Arnold replied that CDC provides technical assistance to state and municipal partners to improve public health infrastructure and data collection efforts, including accurately capturing data on race, ethnicity, and SDOH.

Subcommittee on Standards—Rich Landen and Denise Love, Subcommittee Co-Chairs

Update on Convergence 2.0 Project

The Convergence 2.0 project aims to modernize the standards adoption framework to support current technologies and health care needs, reduce burden throughout the health care system, and harmonize standards across clinical, administrative, and public health data. The Convergence 2.0 project builds on previous work of the Subcommittee on Standards related to the Predictability Roadmap, which was launched to (1) envision industry-driven standards development and adoption, (2) provide timely standards-related updates, (3) enable pre-adoption testing and more value assessments, and (4) enhance conformance with standards.

The Convergence 2.0 project recently completed Phase 1, in which the Subcommittee on Standards assessed the current health data standards landscape by conducting Listening Sessions, reviewing Request for Comment (RFC) submissions, identifying potential solutions, and developing a Phase 2 plan. This project included meetings with the Centers for Medicare and Medicaid Services (CMS) Office of Burden Reduction and Health Informatics (OBRHI) and the Office of National Coordinator for Health Information Technology (ONC) to gain their comments and input. The Subcommittee on Standards is currently in Phase 2, which focuses on developing and refining recommendations based on the information collected in Phase 1 and industry consultations. Based on an industry listening session held in August 2021, review of RFC submissions, and comments from OBRHI and ONC, the Subcommittee on Standards identified the following 10 objectives:

1. Test standards and evaluate return on investment of new HIPAA standards prior to federal adoption
2. Adopt health care attachment standards (e.g., Accredited Standards Committee [ASC] X12, Health Level Seven International [HL7])
3. Adopt a standard for HIPAA Acknowledgement forms
4. Publish the HL7 Prior Authorization Application Programming Interface (API) Regulation
5. Improve regulatory processes for adopting standards under HIPAA (e.g., ONC Standards Version Advancement Process)
6. Implement a patient education campaign on patient applications and data privacy
7. Implement training programs for providers on health data exchange to support bidirectional data sharing
8. Identify, implement, and adopt standards for payers and other organizations to exchange information bidirectionally
9. Develop a universal solution for patient matching/identification across health care systems
10. Consider expansion of HIPAA to entities not currently covered by HIPAA standards, such as organizations that host data from HIPAA covered entities (CEs)

Review of Recommendation Letter to Modernize Adoption of HIPAA Transaction Standards

Background

Based upon the objectives identified by the Convergence 2.0 Project, NCVHS sent recommendations regarding HIPAA standards modernization in a letter to Secretary Becerra in March 2022. These recommendations recognized that the nature of e-commerce and health care delivery have changed since HIPAA's enactment in 1996, and that some components of the HIPAA framework are either outdated or dysfunctional. Many CEs and vendors are using new standards (e.g., Fast Healthcare Interoperability Resources [FHIR], X12) and technologies, and best practices from industry and CEs should be evaluated for broader use across the health care and public health sectors. Furthermore, HIPAA's standards adoption process has become obsolete and requires updates. In June 2022, the Subcommittee on Standards held an industry listening session to discuss five considerations (listed below) for standards adoption and advancement. Industry stakeholders recommended removing Consideration 3 regarding the HIPAA standards exceptions process, but agreed with the other proposed recommendations.

- **Consideration 1:** Update relevant HIPAA policies to allow the adoption and use of more than one standard per business function. Health plans would be required to support all adopted standards for their industry sector. Providers could choose which other proposed/adopted standard or standards to conduct with their health plans.
- **Consideration 2:** Enable HIPAA covered entities to support multiple versions of adopted standards for business functions. This provides an opportunity for innovators to be one version ahead of the current adopted version.
- **Consideration 3:** Revise the standards exception process for HIPAA covered entities that submit an application with the required justification and business case to automatically authorize them without waiting for review. Willing trading partners would automatically be authorized to use different standards for the same transaction and for the same business purpose(s). Reporting on the use of alternative standards would be required of the willing trading partners.
- **Consideration 4:** Identify options for improved integration of health information standards, including base standards plus standard development organization (SDO) implementation guides, more broadly than at present, and fostering relevant collaboration across HHS Agencies and Offices (e.g., CMS, ONC, CDC, NIH, IHS) including State, Local, Tribal & Territorial Governments (STLS).

- **Consideration 5:** Develop and publish a guidance framework with recommended definitions, metrics, templates, and pilot test procedures, including methods for reporting on standards readiness, standards costs, results of real-world testing and metrics essential for evaluation of standards. This would enable better measurement, management, and understanding of standards maturity, standards implementation success, and the net value of standards.

Recommendations and Feedback

Based on these considerations and feedback from industry and government stakeholders, the Subcommittee on Standards proposes four recommendations to be shared with HHS, which are presented below:

Recommendation 1: Update relevant HIPAA policies to allow the adoption and use of more than one standard per business function.

Feedback from industry stakeholders indicated that allowing more than one standard would enable different entities to select which standard best fits their business function and requirements. For example, the American Dental Association (ADA) stated in an August 2021 comment letter that X12 standards are not ideal for dentistry providers and recommended using FHIR standards for HIPAA-covered transactions. However, many health care administrative stakeholders and payers have already adopted X12 standards and transitioning to FHIR could be both burdensome and expensive.

Recommendation 2: Enable HIPAA Covered Entities to support one or more versions of adopted standards for business functions.

HIPAA currently allows only one standard to be in effect at any given time, and when a new version is adopted, all HIPAA CEs must transition to that new standard within the specified transition period. These transitions can be financially and logistically difficult for many smaller entities, which may not see significant efficiencies using the new standards. The Standards Subcommittee recommends enabling some entities to continue to use older versions of standards based on entity-specific requirements.

Recommendation 3: Recognizing ONC's existing authority to facilitate the coordination of SDOH efforts across HHS agencies and offices (e.g., CMS, ONC, CDC, National Institutes of Health [NIH], Indian Health Service [IHS]), HHS should expand ONC's authority to include a formalized public process for convening non-federal entities (State, Local, Tribal & Territorial Governments [STLS]) and to align reporting requirements in federal funding opportunities (e.g., by agencies such as Health Resources and Services Administration [HRSA], SAMHSA, and CMS).

ONC currently coordinates data harmonization and exchange across multiple HHS agencies, including CMS, CDC, OCR, and IHS. HHS can expand ONC's authority to include STLS agencies in order to further harmonize and exchange public health data. Furthermore, aligning SDOH data reporting and exchange across different levels of government enhances HHS's ability to identify and address health disparities within the population.

Recommendation 4: HHS should develop and publish a guidance framework for Standards Development Organizations (SDOs) 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.

SDOs (e.g., HL7, Accredited Standards Committee [ASC]) develop projects and metrics to evaluate the functionality, capabilities, and readiness of different standards. Establishing a guidance framework for standards evaluation would enable public health agencies, SDOs, and health care industry partners to assess the benefits and costs of adopting new standards in a harmonized manner.

Discussion of Recommendations

For Recommendation 3, Ms. Goldstein recommended clarifying the phrase "SDOH efforts" to specify whether this phrase applies to SDOH data reporting, data elements, data standards, or data dictionaries. Ms. Love agreed with the need to clarify ONC's role and suggested that ASPE could develop a central conceptual framework for reporting on SDOH, including data definitions, implementation processes, and health data elements. Mr. Landen clarified that the recommendation is meant to build upon ONC's existing purview for data harmonization and exchange rather than delegating this authority to a different HHS agency.

For Recommendation 3, Dr. Mays recommended changing the phrase "health disparities" to "health inequities" because some disparities exist between populations for reasons not related to systemic inequities. In the description section that accompanies Recommendation 3, Dr. Mays also recommended emphasizing the role of improving health outcomes among disadvantaged populations. Ms. Love agreed to make this change in the final letter.

Dr. Watzlaf asked which HHS agency would establish the standards evaluation framework for SDOs as part of Recommendation 4. Mr. Landen replied that this framework will likely be overseen by OBRHI National Standards Group (NSG). The Subcommittee on Standards has already held initial discussions with NSG about developing a standards evaluation framework. These discussions have emphasized the importance of ensuring that newer versions of standards provide enough value (e.g., enhanced analyses or interoperability) to justify the cost associated with adoption.

Review of Text of Recommendations Letter

Mr. Landen summarized the cover letter, which provides an overview of (1) NCVHS and its role as an advisory body for the HHS Secretary; (2) background for the recommendations, including information collected during listening sessions; and (3) an overview of HHS's purview in overseeing and updating HIPAA transaction standards. Mr. Landen than reviewed the text for the recommendations and accompanying descriptions. In Recommendation 1, the accompanying description describes how HIPAA's requirement for one universal standard was based on the technology available when HIPAA was first passed in 1996. The evolution of technology and information technology (IT) standards during the past 26 years has changed the health IT landscape, and capitalizing on new efficiencies and technologies (e.g., APIs, electronic attachments) requires more than one standard.

Dr. Mays asked whether the phrase "update relevant HIPAA policies" should be changed to "update *specific* HIPAA policies." Mr. Landen replied that the Subcommittee on Standards chose "relevant" to reflect that implementing the Subcommittee's recommendations may require changes to other HIPAA policies not identified by the Subcommittee.

The accompanying text to Recommendation 2 describes the burden of updated versions of health IT standards on many health care providers and industry stakeholders. Some standards updates include new fields that are not required by many components of the health care system, but HIPAA currently requires all CEs to upgrade their systems to the new standard. Allowing CEs to use more than one version of a standard will reduce the cost of upgrades for many industry stakeholders.

Recommendation 3 includes a goal of aligning reporting requirements for federal funding opportunities through HHS agencies (e.g., HRSA, SAMHSA, CMS). Dr. Mays asked whether aligning reporting requirements would be limited to new funding or would include existing programs funded by HHS as part of required program reporting. Mr. Landen replied that this reference to funding includes grants for research, data modernization, health infrastructure upgrades, and other public health funding. Connecting these requirements to funding opportunities enables HHS to consistently apply reporting requirements across STLS public health agencies. Dr. Xu recommended rewording the recommendation to state "health care systems" before funding opportunities for STLS partners. The full Committee agreed with this suggestion and agreed to include language in the description connecting these requirements to data system alignment.

Recommendation 4's accompanying text notes that HIPAA does not currently include an established process for evaluating or testing health IT standards. While some SDOs conduct testing in controlled environments, a consistent and objective evaluation and testing framework would enable regulatory agencies and industry stakeholders to compare benefits and capabilities of different standards.

Status on Proposals on New HIPAA Transaction Standards and Operating Rules

NCVHS has received requests from X12 to review updates to three HIPAA claims transactions implementation guides (i.e., 837 Professional, Institutional, and Dental Claims), as well as the 835 Payment and Remittance Advice implementation guide. X12 recommends the following number of enhancements for each implementation guide: 1,041 for Professional, 1,136 for Institutional, 333 for Dental, and 259 for Payment and Remittance Advice. X12 also proposes to transition from Version 5010 to 8020 of the Transactions Standards. Version 5010 was balloted by V12 in 2003, adopted under HIPAA by CMS in 2009, and implemented by industry in 2012. Version 8020 was balloted by X12 in 2020. The Subcommittee on Standards will soon meet with X12 to receive an overview presentation and will subsequently release a Federal Register Notice (FRN) with RFC and host a 1-day listening session in Q3 2022.

The Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) has submitted a letter to NCVHS proposing (1) updates to three existing rules that have been adopted by CMS under HIPAA (i.e., the Connectivity Rule, Infrastructure Rule, and Eligibility & Benefits Data Content Rule) and (2) two new operating rules (i.e., Attachments Rule and Eligibility & Benefits Single Patient Attribution Data Content Rule). The Subcommittee on Standards will receive a presentation from CAQH CORE during August 2022 and will then release a FRN with RFC and host a 1-day listening session in Q3 2022.

Following both listening sessions, the Subcommittee will then draft recommendations to be shared with NCVHS during the next Full Committee meeting.

Developments in International Classification of Diseases 11th Revision (ICD-11) Transition

ICD-11 was adopted by the World Health Organization (WHO) in May 2019, with the goal of beginning implementation during January 2022. ICD-11 has three components: mortality, morbidity for U.S. health care and public health, and morbidity for U.S. health care billing and payment. NCVHS has submitted a letter of recommendation to HHS, which requests that HHS (1) conduct research to determine how well ICD-11 meets the needs of the United States and (2) develop a communications plan to avoid challenges experienced during ICD-10 adoption. HHS has acknowledged the NCVHS recommendations and some research has been conducted within NIH; however, the research studies recommended by the Subcommittee on Standards have not yet occurred. The Subcommittee has since held conversations with

OBRHI, which, in collaboration with the CMS Division of National Standards, will submit a FY23 budget request seeking funding to conduct the research studies recommended by the Subcommittee.

Ms. Skurka shared that 30 countries have transitioned to ICD-11. In Canada, work is underway to assess transitioning to ICD-11, but no timeline for implementation is available. Canadian authorities are currently assessing whether a Canada-specific version of ICD-11 is required. WHO is discouraging country-specific modifications, however WHO is encouraging suggestions for modifications to be directed to WHO and incorporated broadly to ensure standardization. Australia has not yet made a formal decision regarding transitioning to ICD-11.

Subcommittee on Privacy, Confidentiality and Security – Briefing on Current Issues in Cybersecurity—Moderator: Melissa Goldstein, Subcommittee Co-Chair
The Privacy, Confidentiality and Security (PCS) Subcommittee continues to evaluate cybersecurity concerns, including inviting a panel of experts on cybersecurity and privacy concerns in health IT who provided presentations that are summarized in the sections below:

- ***Greg Garcia, Executive Director, Cybersecurity, Health Sector Coordinating Council***

Health care and public health infrastructure is as classified as "critical infrastructure" under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 and multiple executive orders. This critical infrastructure includes:

- Laboratories, blood, and pharmaceuticals (e.g., pharmaceutical manufacturers, blood banks)
- Medical materials (e.g., medical device manufacturers, medical equipment and supplies)
- Health IT (e.g., electronic medical record systems)
- Federal response and program offices, including coordinated response activities across federal agencies
- Direct patient care (e.g., medical facilities, emergency medical services)
- Mass fatality management services (e.g., coroners, morgues, medical examiners)
- Health plans and payers (e.g., health insurance companies, state emergency health organizations)
- Public health, including governmental public health services and networks

The Health Sector Coordinating Council (HSCC) was established as an advisory committee that provides advice on protecting this infrastructure. The HSCC identifies both cyber and physical risks to health sector security and resilience, develops guidance for mitigating these risks, and coordinates with the federal government to facilitate threat preparedness and incident response. The HSCC Cybersecurity Working Group (CWG) focuses on identifying and developing responses to cybersecurity threats and vulnerabilities in the health care sector and works closely with agencies such as ASPE, the HHS Office of Chief Information Officer, and FDA. As of June 2022, CWG included 318 voting organization members, including 45 industry companies, nine federal agencies, two state agencies, two municipal agencies, and two Canadian government agencies. CWG is overseen by the HSCC Executive Committee, which also oversees multiple other task groups, including 405d Cybersecurity Practices; Emerging Technologies Cybersecurity; Risk Assessment, Workforce Development, and Supply Chain Risk Management. These task groups were created in response to the June 2017 report by the Health Care Industry Cybersecurity Task Force. This report identified the following six imperatives:

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity
2. Increase the security and resilience of medical devices and health IT

3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
4. Increase health care industry readiness through improved cybersecurity awareness and education
5. Identify mechanisms to protect research and development efforts and intellectual property from attacks and exposure
6. Improve information sharing of industry threats, risks, and mitigations

Based on these imperatives, the HSSC CWG has produced 15 best practices guidance documents for health care cybersecurity. The CWG now aims to partner with HHS and other federal agencies to help disseminate these guidance documents throughout the health care community and improve cybersecurity practices across the health care sector. CWG recently met with Chris Inglis, the White House National Cyber Director, to discuss methods to disseminate these tools and best practices.

- ***Andrea Matwyshyn, JD, PhD, Professor of Law and Engineering Policy, Pennsylvania State University***

Concerns regarding data confidentiality, integrity, availability, and security are issues of health care safety, and addressing these issues requires a robust approach that views privacy and security as complementary factors. The importance of privacy and security must be taught to professionals in health care, privacy law, and cybersecurity fields. Many medical schools do not include courses on security principles and the impact of privacy on patient safety. As technologies advance and become increasingly integrated into the Internet of Things (IoT), potential threats to patient safety will increase if not sufficiently addressed.

As it grows, the IoT also increasingly expands into medical devices, including implanted devices and multi-purpose devices for medical and non-medical uses. Many embedded medical devices (e.g., deep brain stimulation) systems connect with back-end data systems, machine learning algorithms, and mobile electronic devices. While FDA increasingly regulates cybersecurity related to medical devices, this regulation does not always extend to these connected systems, leading to risks for security breaches.

- ***L. Reuven Pasternak, MD, MPH, MBA, Senior Advisor, National Risk Management Center, Cybersecurity and Infrastructure Security Agency (CISA)***

The mission of CISA is to partner with industry and government to understand and manage risk to U.S. critical infrastructure, with two major goals: to defend against urgent threats and hazards and to strengthen critical infrastructure and address long-term risks. Through its efforts, CISA protects 55 national critical functions (NCFs), which are government and private sector functions that are so vital to the United States that their disruption or dysfunction would have a debilitating effect on security, national economic security, national public health, or safety. The 55 NCFs be organized into four major sets: (1) connect (e.g., provide cable access network services), (2) distribute (e.g., maintain supply chains), (3) manage (e.g., provide medical care and insurance services), and (4) supply (e.g., supply water). Three of the NCFs within the "manage" set are directly related to health care: (1) maintain access to medical records, (2) provide medical care, and (3) support community health.

CISA aims to instill resilience within the health care sector to help prepare for the impact and stress of future pandemics. To that end, CISA has developed the Cascading Impact of Disruptions model to estimate the cascading effects of a potential COVID-19 surge, which starts with unaffected operations and ends in regional degradation. This model considers changes in hospital capacity and demand over time to address how hospitals can evaluate their options to prevent capacity degradation and possible crises. CISA has also created the Disruptive Event Level System, in which Level 1 indicates normal operations and

Level 5 indicates a system that cannot provide services due to compromised infrastructure. Disruptive events can include resource changes (e.g., shortages), cyberattacks, sudden increases in acute health care demand (e.g., outbreak or mass casualty event), environmental events (e.g., hurricane), or infrastructure events (e.g., loss of power).

- ***Linda Ricci, MME, MPH, Director, Division of All Hazards Response, Science and Strategic Partnerships, FDA***

Medical devices are a critical component of the health sector ecosystem and thus FDA is working to ensure that approved devices apply necessary cybersecurity practices. FDA's Center for Devices and Radiological Health enforces a total product lifecycle approach that involves cybersecurity engineering and post-market vulnerability management to prevent cybersecurity flaws, which can lead to unavailability of resources, such as health care records, databases, devices, and systems needed to facilitate typical health care practices. Medical devices belong to the class of operational technology (OT), not information technology, and OT cybersecurity risks are growing. OT cybersecurity must be a shared responsibility across state and federal governments as well as the private sector (including security research firms, patient groups, medical device trade groups, and physician societies).

FDA has prevented several devices from coming to market based on cybersecurity alone. Cybersecurity directly impacts patient safety and thus FDA has continuously supported the development of cybersecurity guidance documents related to premarket submissions and post-market products. A revised draft premarket guidance document was released for comment during April 2022. This revised draft includes more detailed technical recommendations on premarket documentation for cybersecurity risk and recommendations on Software Bill of Materials (SBOM) and alignment with Executive Order 14028, and eliminates some risk tiers. Conducting cybersecurity evaluations early in the premarket review process prevents at-risk devices from becoming legacy devices once cybersecurity flaws have been realized, possibly after the devices have already been disseminated to hospitals.

FDA has also recommended A-19 legislative actions for medical device cybersecurity. Currently, no statutory requirement requires medical device manufacturers to address cybersecurity. FDA's draft A-19 establishes explicit cybersecurity requirements, including that (1) SBOM will be used to track third-party risk of software cybersecurity vulnerabilities, (2) devices must have the capability to be updated and patched in a timely manner, (3) manufacturers must demonstrate reasonable assurance of a device's safety and effectiveness for purposes of cybersecurity, and (4) manufacturers must have coordinated vulnerability disclosure policies for public notification when a manufacturer learns of a cybersecurity vulnerability within a medical device.

Discussion

Ms. Monson asked what additional efforts the PCS Subcommittee can pursue to help support the cybersecurity work presented by panelists in this session. Ms. Ricci suggested that the PCS Subcommittee continue to promote cybersecurity awareness and the importance of upholding expectations related to cybersecurity within the health care sector. Mr. Garcia added that the Subcommittee could help support HSCC work by encouraging the broad use of HSCC resources, such as the Health Industry Cybersecurity Practices, and improving the health care cybersecurity workforce through increased training. Dr. Matwyshyn recommended that the Subcommittee encourage the use of (1) the Playbook for Threat Modeling Medical Devices developed by the MITRE Corporation, (2) guidance documents developed by the Department of Justice's Computer Crime and Intellectual Property Section detailing methods of corporate conduct that improve resilience to cyberattacks, and (3) International Organization for

Standardization (ISO)/International Electrotechnical Commission (IEC) documents ISO/IEC 29147 and ISO/IEC 30111. Dr. Matwyshyn also suggested that the Subcommittee support more funding for (1) medical professional curricular development through CDC or HHS to help medical and engineering schools incorporate cybersecurity training and (2) a first responder-style program for cybersecurity attack preparedness in the health care sector.

Dr. Watzlaf asked Dr. Matwyshyn for additional sources of guidance on how embedded medical devices should be regulated. Dr. Matwyshyn recommended reviewing her publication entitled "The Internet of Bodies," which can be found in the *William & Mary Law Review*.

Dr. Mays asked panelists which institutions—possibly institutional review boards, medical and engineering schools, hospitals, device developers, or NIH—should be responsible for ensuring cybersecurity compliance within the health care and research fields. Panelists noted that maintaining cybersecurity compliance and awareness must be a shared responsibility for all entities involved in the health care sector. Dr. Matwyshyn suggested developing a cross-agency task force that identifies the regulatory core competencies of each agency, how they relate, and how they can be used to address the universe of concerns and issues related to health care cybersecurity; such a task force could also lead agencies to collaborate on common priorities and competencies related to cybersecurity.

Noting the increasing commonness of telehealth practices, Ms. Banks asked panelists how to approach cybersecurity practices for data shared among patient homes, hospitals, and payers. Panelists emphasized the development of "zero-trust architecture" and threat-level modeling, as well as educational materials for all stakeholders.

Public Comment—Rebecca Hines, Executive Secretary and Designated Federal Officer

Mr. Ogi Kwon of R1 Revenue Cycle Management noted the lack of payer portal direct data entry regulatory recommendations during today's presentations and asked whether this topic remains a priority to NCVHS. Mr. Kwon observed that this topic was noted as a priority during the 2021 NCVHS listening session and the January 2022 NCVHS Full Committee meeting. Mr. Kwon added that payer portals are administratively burdensome for providers to navigate and often include highly restrictive terms of use.

Ms. Hines read a comment received prior to the Public Comment period that pertained to the second Subcommittee on Standards recommendation and included a question regarding whether the Subcommittee has identified a timeline for transitioning to updated systems.

Mr. Mike Denison of Change Healthcare notified NCVHS that he shared several comments via email.

Wrap Up and Adjourn—Jacki Monson, Chair

Ms. Monson thanked attendees for their participation and adjourned until the following day.

—DAY TWO—

Call to Order and Roll Call—Rebecca Hines, Executive Secretary and Designated Federal Officer

Ms. Hines invited NCVHS Committee members and speakers to introduce themselves and disclose any conflicts of interest. No attendees stated a conflict of interest for today's meeting.

Welcome Remarks and Agenda Review—Jacki Monson, Chair

Ms. Monson welcomed NCVHS Committee members and invited speakers to the meeting and reviewed the meeting agenda.

Workgroup to Assess Sexual Orientation and Gender Identity (SOGI) and Social Determinants of Health (SDOH) Data and Measures Definition, Collection, and Use – Update—Vickie Mays, Workgroup Co-Chair

The SOGI/SDOH Data Workgroup's efforts reflect the Biden-Harris administration's priority to address health and well-being inequities. President Biden recently issued executive orders specifically addressing inequities for SOGI minorities. In June 2022, President Biden noted that more than 300 laws have been introduced in state legislatures within the last year that target the rights of lesbian, gay, bisexual, transgender, and intersex (LGBTQI) individuals. The vast majority of these bills target transgender and nonbinary children and their parents, including bans on health care services. The Biden-Harris administration has encouraged HHS agencies to address health and well-being inequities and discrimination affecting LGBTQI children and families and to issue guidance to states and municipalities on expanding comprehensive health care access for LGBTQI individuals. Developing this guidance requires reliable SOGI and SDOH data that capture current disparities and barriers to health care access; NCVHS is ideally suited to recommend changes to improve the collection and accuracy of SOGI and SDOH data in order to support the goal of reducing health disparities. To improve SOGI and SDOH data collection, NCVHS charged the SOGI/SDOH Data Workgroup with the following objectives:

- Identify considerations and options to define methodologically sound categories for framing sources of SOGI and SDOH data (e.g., survey, administrative, clinical, vital records, and public health surveillance)
- Identify domains of SOGI and SDOH data that should be collected by data category, including suggestions for domain prioritization in the case that only limited data can be collected
- Conduct an assessment of best practices regarding how SOGI and SDOH data should be collected, including specific data elements, data standards, the order of questions, public trust, and alternatives to improve data equity and equitable evidence-based decision-making
- Provide findings to NCVHS regarding privacy considerations for use and linkage of SOGI and SDOH data (e.g., administrative, clinical, public health, and research purposes)

Dr. Mays emphasized the importance of public trust in NCVHS and other public health agencies when collecting accurate SOGI and SDOH data. Since SOGI and SDOH data often involve sensitive and personal information, a lack of trust among the public during the collection and usage of these data can lead to inaccurate data, thus reducing data quality and usefulness for decision-making. Ensuring SOGI and SDOH data quality and integrity also requires adapting data collection processes as definitions change over time. In addition, establishing robust privacy protections and the perception of privacy is also crucial for collecting and using SOGI and SDOH data. Ensuring the perception of data privacy requires consideration of the potential harms of collecting SOGI and SDOH data and establishing boundaries to prevent misuse of sensitive data or accidental disclosure of an individual's data. In jurisdictions that prohibit gender-affirming care for minors, disclosure of health data (including treatments such as hormone replacement therapy) can reveal minors who are receiving gender-affirming care, resulting in legal action by that jurisdiction against the minor's parents. These concerns cause many SOGI minorities to avoid disclosing relevant data about health equity and disparities, which may lead to underestimates of health disparities.

Dr. Mays posed two questions to NCVHS members:

1. What issues have members observed around the collection and usage of SOGI and SDOH data?
2. Because federal agencies use SOGI and SDOH data for different purposes, what are some use cases that illustrate the needs and applications for these data?

Discussion

Ms. Love noted that many states and jurisdictions are seeking federal guidance regarding the proper collection and usage of SOGI and SDOH data, including which data elements are clinically relevant, potential proxy measures for assessing disparities and risk, and how to identify data bias and inaccuracies. NCVHS can play a role in assisting HHS by issuing proactive guidance to states and jurisdictions on SOGI and SDOH data collection in order to improve data quality and analyses of health disparities.

Dr. Xu recommended focusing the Workgroup's actions on tangible deliverables that NCVHS can provide to HHS to aid the nationwide effort toward identifying and addressing SOGI health disparities. For example, the Workgroup can employ a focused approach of developing guidance for several specific use cases rather than developing broad guidance that covers all use cases and settings. Ms. Love agreed with this use case-focused approach and recommended state-specific use cases for states that base payments and incentives upon quality of care. Guidance from HHS can help these states identify quality of care indicators for measuring health inequities.

Ms. Goldstein noted that privacy sensitivity and concerns can differ among historically marginalized populations. Therefore, the Workgroup's efforts to collect accurate SOGI and SDOH data must include continual engagement with underrepresented and historically marginalized groups for their feedback regarding privacy concerns and level of protections needed. HHS and other federal agencies need to continually communicate with these groups to assess changing needs and concerns.

Dr. Mays thanked the Workgroup members for their efforts thus far in identifying high-priority gaps and recommendations and noted that the Workgroup will resume its efforts in fall 2022.

Briefing on Legislative Developments in Data Privacy—Moderators: Melissa Goldstein and Valerie Watzlaf, PCS Subcommittee Co-Chairs

The PCS Subcommittee remains apprised of evolving privacy legislation developments, including inviting a panel of experts on consumer and personal data privacy in the United States and internationally who provided presentations that are summarized in the sections below:

- ***Kristin Cohen, JD, Federal Trade Commission (FTC)***

The FTC is responsible for ensuring the privacy of consumer health data held by entities not be covered by HIPAA, such as data stored in smartphone applications or connected devices as well as data that can be inferred from purchase and location histories. The FTC is a civil law enforcement agency mandated to enforce Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." For example, the FTC recently oversaw a case regarding a smartphone app for tracking menstrual cycles that deceptively sold user data, including inferred pregnancy status, to third-party marketing and analytics entities while falsely stating to consumers that such information remained confidential. In 2021, the FTC issued a policy statement about the coverage of the Health Breach Notification Rule, which requires commercial entities to notify the FTC and affected individuals in the event of a breach of health information. The policy statement emphasized two points: (1) the FTC views most health apps and connected devices as covered by the Rule; and (2) breach of

health information includes events in which a consumer's health information has been disclosed without their authorization as well as external cybersecurity breaches. The FTC further issued a blog post ("Location, health, and other sensitive information") reinforcing its commitment to protecting reproductive health data that, if shared, may be used against consumers following the Supreme Court's decision in Dobbs v. Jackson Women's Health Organization. Given the increasing power of technology to re-identify data, particularly datasets that include location information, de-identified data with location information may not be truly anonymous. FTC Chair Lina Khan will announce an Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security.

- ***Stacey Gray, JD, Future of Privacy Forum***

Privacy laws in the United States have evolved since Congress passed the Privacy Act of 1974, which was the first statute enacted to establish the use and security of consumer information collected by the government. This act originally applied to private companies as well but was later amended to only cover government entities. HIPAA was enacted in 1996 to provide protections for health information, and HIPAA does not fully preempt state laws and regulations regarding health data protections. Despite these advances, the United States lacks universal legislation that covers all personal information, health or otherwise, regardless of origin or intended use. As a result, personal information, including internet browsing and purchase history, is largely unregulated compared to health information, even though third parties may often infer health information (e.g., medical conditions) from unregulated consumer data (e.g., internet search history). Federal lawmakers were unable to pass the Consumer Privacy Bill of Rights Act of 2015, though California lawmakers were later able to pass similar legislation in the California Consumer Privacy Act (CCPA) of 2018. Due to the size of California's population and economy, the CCPA effectively became a national privacy law. However, complying with the CCPA presents challenges due to ambiguities in the original bill compared to the more comprehensive European Union (EU) General Data Protection Regulation (GDPR) of 2016, which regulates and protects personally identifiable information.

Similar consumer privacy legislation has since passed in Virginia and Colorado in 2021 as well as in Utah and Connecticut in 2022. Most state consumer privacy legislation has mirrored the CCPA in both scope and core consumer rights, regulating all business entities doing business in the respective states with exceptions for small businesses with lower revenues. The Colorado Privacy Act extends the scope of regulation to include academic and nonprofit entities, which have largely been exempt from any consumer privacy regulation nationally. Each of these states defines consumer data broadly as any information directly or indirectly related to an identified or identifiable natural person (under CA law) or resident (under CO, UT, CT, and VA law) of that state. This includes information typically considered identifiable (e.g., name, address, age) as well as information less frequently considered identifiable, such as internet browser history, device identification number, and Internet Protocol (IP) address. Individual consumer rights guaranteed include the right to request and receive access to their data, delete that data, and, in some states, modify that data. Legislation in several states, modeled after the CCPA, further guarantees consumers the right to opt out of data collection and the sale of their data to third parties such as marketing and analytics firms. Most states with consumer privacy legislation have also codified additional higher standards for sensitive data, such as health conditions, diagnoses, sexual orientation, race/ethnicity, and religion, that require affirmative expressed consent to collect. State legislation on consumer privacy is enforced by the respective state attorney general, though consumer rights groups advocate for increased enforcement through civil liability with the ability to bring lawsuits against entities in violation. California has taken privacy enforcement further by establishing the California Privacy Protection Agency, which is the first dedicated privacy protection agency. This agency has administrative and enforcement authority regarding the CCPA, including the ability to establish draft privacy regulations

based on public comments. Other states may incorporate similar legal measures, including establishing agencies or other provisions, to strengthen privacy regulations enforcement.

- ***Lauren Riplinger, American Health Information Management Association***

The scope of health information has expanded with an increasing number of consumer-facing technologies, applications, products, and services not covered by HIPAA. Health information professionals face difficulty in navigating and complying with the patchwork of state and federal laws that govern protected health information. While state and federal legislation seeks to regulate the use and flow of health information, governmental agencies such as CMS, ONC, and HHS have each enacted additional policies that govern the use and sharing of health information:

- The CMS Promoting Interoperability Program and the Interoperability and Patient Access Rule respectively work to enhance providers' abilities to share health records with other providers and patients' access to their own health information.
- ONC's 21st Century Cures Act Final Rule further facilitates patient data requests, improving patients' access to their health information.
- The HHS No Surprises Act protects patients from surprise medical bills from out-of-network providers that may be incurred during emergency medical interventions and procedures.

HHS and CMS work further to improve hospital, provider, and health plan price transparency for medical bills. Lawmakers and their constituents grow increasingly interested in comprehensive privacy legislation, enforced by the FTC, with the hope that Congress will catch up to states that have already passed consumer privacy legislation (CA, CO, CT, UT, VA).

To provide nationwide data privacy protections, the U.S. House of Representatives introduced H.R. 8152 – American Data Privacy and Protection Act (ADPPA) in June 2022 with strong bipartisan and bicameral support, and ADPPA is currently under consideration by the 117th Congress. This legislation would address not only health data but all "information identifying, linked, or reasonably linkable to an individual or device linkable to an individual," excluding de-identified data, employee data, and publicly available information. Sensitive data covered by the ADPPA, including identifiable health data, would be subjected to heightened requirements. Covered data subject to other federal data protection laws (e.g., HIPAA-covered data) are intentionally exempted from this legislation, provided that said covered data are used in compliance with those laws. Legislators are negotiating two key areas of the ADPPA: (1) federal preemption of state laws, and (2) private right of action (i.e., when a private citizen/person is legally entitled to enforce their rights under a given statute).

If ADPPA is enacted, NCVHS may need to determine what data may be covered by both HIPAA and ADPPA. Similarly, NCVHS may also focus on approaches to de-identification of health data to protect individuals' privacy and data security while ensuring sufficient data availability and liquidity for public health purposes.

- ***Cobun Zweifel-Keegan, JD, International Association of Privacy Professionals***

The United States and the EU have developed privacy regulation legislation in parallel, but approach privacy differently from one another: the EU's GDPR treats personal privacy as an extension of human rights, whereas the United States frames privacy rights as an extension of consumer protection from the perspective of privacy torts, in which civil courts impose liability for breaches of privacy and damages or harm caused by such breaches.

The EU's GDPR of 2016 was the first to codify enforcement standards for privacy violations. The GDPR also accelerated the implementation of privacy best practices by entities not only operating within the EU but also globally. Since the EU passed the GDPR, more than 100 countries have enacted comprehensive privacy legislation and regulations. Internationally, most countries debate and negotiate with one another to regulate the flow of personal data between nations. These negotiations trend in two opposite directions, variously resulting in (1) restrictions that lead to more localized storage and intranational use of data and (2) less restrictive, open flows of data between nations. Russia and China tend to regulate information using the former, localized approach, whereas the EU tends to use bureaucratic structures to allow open flow of information between nations and jurisdictions with similarly high data protection standards and policies. Negotiations between countries that adhere to opposing standards require the formation of data security accountability structures with a minimal level of foundational agreement between both parties sharing data.

In the Asia-Pacific region, the dominant concept of "data free flow with trust" is based on the mutual trust among nations in the region and the agreement that nations sharing data will offer flexibility to adapt to nations with higher standards of data privacy protection. The U.S. Department of Commerce advanced the concept from a regional system to a global system by expanding the Cross-Border Privacy Rules (CBPR) System from the Asia-Pacific Economic Cooperation to allow the participation of countries outside the Asia-Pacific region.

Other countries are also updating their data privacy protections. The United Kingdom began shifting its data protection policies toward a localized approach after exiting the EU. Canada and Costa Rica are in the process of updating their national policies around data privacy protection, and Brazil recently began enforcing its own national omnibus bill on data privacy protection. In addition, China is finalizing multiple sets of comprehensive privacy standards and strict data transfer requirements. The EU remains a leader in developing and modernizing data privacy protections, including protections regarding how artificial intelligence and other new and emerging technologies may impact the flow and security of personal information. Many of these proposed regulations apply more broadly to antitrust law as well.

Discussion

Dr. Watzlaf requested that speakers share their perspectives on the topics on which NCVHS advice to HHS would be most timely and constructive. Ms. Riplinger shared that a better understanding of the intersection of HIPAA and other privacy regulations (e.g., ADPPA) would be especially relevant. Entities that are partially or completely exempt from HIPAA may be concerned about maintaining compliance as privacy policy and regulations evolve. HIPAA will also require revitalization to remain current with developments in technology that increasingly collect more personal data from users. Mr. Zweifel-Keegan shared that organizations frequently request or would benefit from guidance and recommended best practices from regulators. Ms. Gray added that HHS could provide guidance on how commercial partnerships and commercial data-driven research can comply with evolving privacy regulations, including when commercial partnerships include academic institutions. Academic institutions and research partners face external pressure to conduct social research on topics such as social media use and mental health, which often require access to underlying commercial data. Gaining access to this underlying data can conflict with business entity policies or interests. Some private companies also have a commercial interest in the development of privacy-enhancing technologies, which would in turn require updated national standards on de-identification of data that may also facilitate ethical social research efforts.

Ms. Goldstein highlighted the relevance of sector-specific exemptions in HIPAA that may complicate those entities' understanding of how various state and federal policies apply to collected personal information,

especially for entities that are not covered by HIPAA but still collect health information such as genetic and biometric information. Sectoral exceptions in HIPAA are primarily based upon the type of data collected rather than the industry or sector to which the entity belongs. State legislators sometimes confuse data type and entity type in initial drafts of proposed privacy legislation. However, data type, (e.g., covered health information, personally identifiable information) takes precedence over entity type, and entities outside of the health sector that collect health information should theoretically not be exempt from regulation by HIPAA, other federal privacy policies, or local privacy policies at the state level. Ms. Cohen added that the FTC has concurrent jurisdiction over some entities covered by HIPAA, providing examples of cases where the FTC brought cases against several chain pharmacies. The FTC exempts many nonprofit, banking and insurance entities from other privacy regulations overseen by the FTC, although this may change with the potential passage of the ADPPA and other state and federal legislation in the future. EU privacy polices account for data type, entity type, and the relationship between the data subject (i.e., the individual supplying the data) and the entity that is processing the data.

Dr. Mays echoed Ms. Cohen's point about the potential re-identification of de-identified data and requested specific recommendations from presenters about improvements that could be implemented to protect sensitive information, such as a person's sexual orientation, gender identify, or SDOH. Ms. Cohen concurred that de-identification of data is both difficult and important, especially related to information that could be used to identify an individual's SOGI and SDOH. In the FTC's 2012 Final Commission Report, the Commission not only emphasized the importance of de-identifying consumer data to a reasonable level, but also advocated for the entities holding or using de-identified data to publicly commit to not re-identifying that data. Ms. Cohen cautioned that entities often attempt to alleviate public privacy concerns by claiming that consumer data will be anonymized, but the entity retains information that can readily re-identify such data. The FTC tightly monitors this type of deceptive trade practice and actively pursues culpable entities. Mr. Zweifel-Keegan added that, in reviewing HHS and OCR guidance on de-identification of sensitive data, he found that many of the guidelines available were developed in 2012 and may benefit from review and updates.

Ms. Love asked Ms. Riplinger how the ADPPA would affect the ONC's Trusted Exchange Framework and Common Agreement (TEFCA). Ms. Riplinger responded that the ADPPA is still in the early stages and may meet further opposition or modification if it passes the House of Representatives for consideration by the Senate. The final provisions of ADPPA will determine whether TEFCA needs to be amended.

Tribal Epidemiology Centers (TECs): Data Access and Privacy—Moderators: Vickie Mays, SOGI/SDOH Data Workgroup Co-Chair, and Valerie Watzlaf, PCS Subcommittee Co-Chair

NCVHS is dedicated to addressing issues of data quality, access, use, and privacy that affect American Indian and Alaska Native (AI/AN) individuals. Dr. Mays thanked speakers for their participation and presentations, which are summarized in the sections below.

- ***Rachel Seeger, MPA, Senior Communications Specialist, OCR***

Ms. Seeger acknowledged the important contributions of the late Ms. Sallie Milam, a former PCS Subcommittee member. Ms. Milam is survived by her long-lasting legacy in data privacy efforts and development of linkages across federal, state, local, Tribal, and private health organizations. Ms. Seeger emphasized that Ms. Milam's thoughtful perspective and passion will be missed at NCVHS.

- ***Kirk Greenway, PhD, Principal Statistician, IHS, and Heather H. McLane, MBA (Yupik) (Kanaka Maoli), Senior Official for Privacy, IHS***

IHS is an HHS agency responsible for providing federal health services to AI/AN individuals. IHS provides a comprehensive health care service delivery system to approximately 2.6 million AI/AN individuals who belong to 574 federally recognized Tribes across 37 states. IHS has developed several IHS Gold Books, which serve as the ultimate resource on the history and objectives of IHS and can be found on the IHS website.

TECs are IHS-funded organizations that serve AI/AN Tribal communities by managing public health information (PHI) systems, investigating diseases of concern, managing disease prevention and control programs, responding to public health emergencies, and coordinating activities with other public health authorities. IHS has established 12 TECs (one for each IHS area and one for urban areas). Reauthorization of the Indian Health Care Improvement Act (IHCIA) acknowledged these TECs as public health authorities. In addition, IHCIA directs the HHS Secretary to grant each TEC access to data, datasets, monitoring systems, delivery systems, and other PHI within the possession of the Secretary.

During a 2007 HHS Tribal consultation session, IHS officials developed a TEC data sharing agreement (DSA) template that aims to standardize DSAs between TECs and IHS Area Offices and ensure regulatory compliance with HIPAA. This DSA template also provides TECs with access to deidentified data from the IHS Epidemiology Data Mart (EDM)/National Data Warehouse for public health surveillance and enables Tribe-specific reporting on community health status. Ten of the 12 TECs have signed DSAs and nine currently use the EDM. The EDM can provide two main types of deidentified data tables quarterly, semiannually, or annually: (1) patient registrations, which include information about patients' AI/AN status, Tribal affiliations, communities of residence, and other demographic information as well as the facilities at which patients are registered, and (2) patient encounters, which includes information about patients' visits (e.g., diagnoses, procedures, result codes, and encounter type).

- ***Kristin Ekelund, MSSA, Senior Analyst, Government Accountability Office (GAO), and Tricia Roy, MPA, Senior Analyst, GAO***

GAO published a report in March 2022 entitled "Tribal Epidemiology Centers: HHS Actions Needed to Enhance Data Access" (GAO-22-104698). The goals of this report were to (1) describe TECs' access to and use of HHS and state epidemiological data and (2) to examine factors that have affected this access and use. To develop this report, GAO reviewed various documents, including reports published by the 12 TECs, DSAs, and CDC and IHS responses to TEC data requests, and interviewed officials from CDC, IHS, and the 12 TECs.

Based on these reviews and interviews, GAO observed that different TECs' access to epidemiological data varied significantly as of November 2021. All TECs have access to data that HHS and states make publicly available (e.g., CDC COVID-19 case data at state and county levels or data on births, deaths, and cancer diagnoses), but some TEC officials had access to additional data types (e.g., vaccination data). Officials from all 12 TECs described challenges accessing data from CDC, IHS, and states. GAO found that TECs used available epidemiological data to conduct a range of analyses to support Tribal decision-making. These analyses were conducted for and at the request of the Tribes, Tribal organizations, urban Indian health programs, and IHS. TEC officials shared that their access to data influenced the specific types of analyses they were able to conduct.

GAO also found that four factors affected TECs' access to and use of HHS epidemiological data: (1) data sharing systems (e.g., HHS Protect and EDM) and agreements help facilitate access; (2) the health care field's lack of policies, guidance, and procedures hinder access; (3) data quality and timeliness affect TECs' use of data; and (4) TECs' capacity can affect their access to and use of data. TECs have been unable to access certain types of data (including data on nationally notifiable diseases, like influenza) because data sharing agreements either have not been established or do not meet the needs of the TECs. The lack of policies and guidance has led HHS officials not to recognize TECs as public health authorities that are authorized to access data, leading to delays in receiving CDC and IHS data and complicating TEC support of Tribal and community leaders. Guidance is also lacking related to how TECs submit data access requests and how agencies should respond to those requests, leading to unclear and inconsistent communications. TECs indicated that having better access to higher quality data would enable them to use resources more efficiently and conduct more impactful work for their Tribes.

GAO recommends that HHS develop a policy clarifying the HHS data that must be made available to TECs as required under federal law. GAO also recommends that CDC and IHS (1) develop written guidance for TECs on how to request data and (2) develop and document agency procedures on reviewing TEC requests and making data available to TECs.

- ***Abigail Echo-Hawk (Pawnee), MA, Director, Urban Indian Health Institute (UIHI)***

Established in 2000, UIHI is the only TEC focused on the needs of urban-dwelling AI/AN individuals. More than 70 percent of AI/AN individuals do not live on Tribal lands, and approximately 70 percent of those individuals live in urban settings. The UIHI Board includes representatives from urban AI/AN communities and leaders across the United States, and UIHI supports 42 organizations operating more than 60 IHS-funded clinics that focus on serving urban AI/AN populations. At the same time, UIHI recognizes that many areas with urban-dwelling AI/AN do not have open clinics because of chronic underfunding (caused by continuous lack of appropriate data capture and collection efforts) and non-fulfillment of treaty rights by the U.S. Government. UIHI also trains epidemiologists on methods to perform small-population analyses—instead of traditional analyses of large datasets—to avoid the statistical insignificance label that frequently plagues the AI/AN community.

Ms. Echo-Hawk emphasized the importance of engaging in current and continuous Tribal consultations, noting that the 2007 Tribal consultation is no longer current or applicable to the contemporary needs of TECs, and underscored the need to implement the recommendations outlined in the GAO presentation. The immense challenges in data access, as well as the low quality of available data, lead directly to a lack of necessary health care analyses and guidelines for AI/AN communities and contribute to the deaths of community members; thus, progress in data access, quality, and sharing are of paramount importance to AI/AN communities and TECs. Ms. Echo-Hawk recommended that the HHS Secretary include Tribal nations and Tribal public health authorities (including TECs) as an adequately resourced part of national data modernization efforts.

- ***Jerilyn LeBeau Church (Mniconjou Lakota), MSW, Chief Executive Officer, Great Plains Tribal Leaders' Health Board***

Many TECs, including the Great Plains TEC, have long observed difficulties in obtaining high-quality health care data for Tribal communities, and these difficulties became more apparent during the COVID-19 pandemic. For the Great Plains TEC, data sharing challenges are compounded by serving Tribal communities across four states: each Tribal community has unique needs, and each state may have different data sharing constraints and policies. Many Tribes served by the Great Plains TEC are Direct

Service Tribes (i.e., they receive care directly from IHS) that rely on the Great Plains Tribal Leaders' Health Board for advocacy, administrative services, and support for accessing health care data from IHS. Recently, the Great Plains Tribal Leaders' Health Board's medical epidemiologist was contacted by a Tribal official who described significant challenges in using community-level COVID-19 vaccination data. The official received the percentage of the community that has been vaccinated but cannot analyze that number by age, gender, or other demographic information to identify which communities must be contacted, educated, and encouraged to obtain a COVID-19 vaccination. In addition to the COVID-19 pandemic, the Great Plains TEC's epidemiology teams are also currently addressing a syphilis outbreak and Tribes are requesting related information from IHS and states to inform case investigation and treatment strategies. However, states have responded with requests for written justifications for the data access requests. IHS freely provides public health data to states, but these data are routinely kept from TECs and Tribal communities. Ms. Church emphasized the need for universal guidance to direct states and agencies on how to share data with TECs and directly with communities, as recommended by GAO.

Discussion

Ms. Echo-Hawk emphasized the importance of standardizing definitions for AI/AN and Tribal identity. Currently, the definition of AI/AN is variable and can include Pacific Islander and Asian communities in some states, resulting in public health data that are confusing or difficult to use. Many Tribal communities are also working to include Tribal affiliation within public health information, but this affiliation must be documented and used appropriately in ways determined through Tribal consultation. Instead, the Northwest TEC, for example, has found that up to 40 percent of AI/AN individuals are either not classified or misclassified as another category. One strategy to reduce misclassifications is to improve training requirements for those classifying individuals at birth and death.

Ms. Roy confirmed that IHS and CDC concurred with the recommendations posed in the GAO report and that GAO anticipates that this concurrence will lead to actions taken to implement the recommendations; GAO will follow up on and monitor progress related to implementing these recommendations.

Dr. Xu asked TEC representatives to share their methods for obtaining funding for data modernization practices. Ms. Echo-Hawk confirmed that very few investments have been made in this area, but that IHS has invested in updating the current EDM data collection systems. Ms. Echo-Hawk added that the current data resources her team is able to extract from the EDM are essentially unusable due to low quality.

Participants discussed whether DSAs are necessary for sharing and transferring data from health care agencies to TECs and Tribal communities, noting that these agreements are intended to help facilitate data access but rarely do so. Participants noted that such agreements should be unnecessary because TECs are authorized public health authorities that deserve the ability to share data in formats helpful to the communities they serve.

Public Comments

Dr. Yvette Roubideaux, Director of the National Congress of American Indians Policy Research Center, emphasized the importance of treating TECs as public health authorities and the disappointment that—even 12 years after this designation—difficulties persist in securing recognition of this status and the associated data access. Dr. Roubideaux stated that the Biden Administration must correct these issues in a timely manner so they do not continue to hinder AI/AN communities' access to critical health data. She added that NCVHS should create a list of priorities that the administration must achieve in order to

reduce these challenges. Dr. Roubideaux added that TECs field significant epidemiological expertise that can be shared with data scientists at HHS.

Ms. Margaret Egan, who serves as general counsel for the Great Plains Tribal Leaders' Health Board, shared that the Great Plains TEC is working to establish an American Indian registry to correct racial misclassifications in state databases. Ms. Egan added that the DSA negotiations between IHS and the TEC that are necessary to complete this registry have been difficult and have taken a significant amount of time. Other TECs have obtained similar data through a simple agreement execution because their state health departments appropriately recognized them as health authorities.

Ms. Michelle Jester, who serves as the Executive Director of SDOH at America's Health Insurance Plans (AHIP), noted that many efforts throughout the health standards space—including the Social Interventions Research & Evaluation Network (SIREN) Gravity Project—have led to the development of standards for SDOH and other demographic data for use in clinical settings. AHIP has worked to map those data standards to existing structures, including FHIR, ICD, Logical Observation Identifiers Names and Codes (LOINC), and Systematized Nomenclature of Medicine (SNOMED).

Mr. Nick Hill, who serves as Lead Epidemiologist for the Great Plains Tribal Leaders' Health Board, noted that both federal and state resources are not always sufficient or appropriate resources to address local needs and outbreaks and thus a decentralization of health data must occur to enable these data to reach local health authorities during emergencies. Mr. Hill added that data modernization efforts must include TEC and AI/AN community leaders to ensure that these efforts are informed by community needs.

Subcommittee on Standards—Rich Landen and Denise Love, Subcommittee Co-Chairs

Final Review of Recommendation Letter to Modernize Adoption of HIPAA Transaction Standards

Ms. Love presented the latest draft of the recommendations letter related to modernizing adoption of HIPAA standards, which was updated based on comments received during Day 1 of this meeting. Many of the changes involved simple wordsmithing (e.g., substituting "needs to" for "should") and reconfigured language, rather than substantive edits.

Recommendation 1

Under Recommendation 1, the Subcommittee reorganized the bullet points to provide examples later in the list but did not change the language of the bullets. Mr. Ferguson recommended removing the phrases "less complex" and "more complex" from the contextual language accompanying the recommendation and updating that language to the following: "A second example, as pointed out in the American Dental Association public comment letter would be to allow some stakeholders to use API standards based on HL7 Fast Healthcare Interoperability Resources (FHIR) while larger organizations could use X12 standards." Mr. Ferguson also recommended including language within the Recommendation 1 rationale related to improving workforce availability and lowering testing costs, such as "The advantages of FHIR for some stakeholders can include better workforce availability, lower total labor costs, or technical tooling compatibility."

Recommendation 2

Under Recommendation 2, the Subcommittee moved some language previously included in the bulleted list to the contextual language accompanying the recommendation.

Recommendation 3

The Subcommittee and NCVHS members updated Recommendation 3 to the following: "NCVHS recommends that HHS expand ONC's existing authority to facilitate the coordination of Social Determinants of Health (SDOH) data standards efforts across HHS agencies and offices (e.g., CMS, ONC, CDC, NIH, IHS), to include a formalized public process that would include non-federal entities (e.g., private health and healthcare systems and State, Local, Tribal & Territorial Governments [STLS]) to align national standards with evolving and complex national and local reporting and information needs."

Participants also agreed to update language in the bullet points to refer to "specific use cases in response to needs" instead of "missing use cases" and to state the following: "To fulfill the intention of this recommendation, the public process needs to include provision of technical assistance to national, STLS, front-line health care workers, and tools (e.g., a virtual EHR for testing purposes, centralized repository of SDOH definitions and formats). Other activities should be identified through this process to accelerate and improve new standards implementation and the integration of SDOH capable of supporting sub-population and social risk and social vulnerability analytics."

Participants also updated the rationale language for Recommendation 3 to the following: "This expanded ONC authority could provide national leadership and establish a centralized venue and process to achieve the objectives for a cohesive process and common base of standards across federal, industry, state, local, and Tribal users to facilitate harmonization, develop needed tools (e.g., a virtual EHR for testing purposes) and provide educational resources for stakeholder engagement."

Recommendation 4

Participants recommended updating the language of Recommendation 4 to state "measures" instead of "quantifiable estimates." The Subcommittee added the following bullet point to the language following Recommendation 4: "In order to streamline and facilitate the regulatory impact and fiscal impact analyses required as part of CMS' rule development processes, the framework needs to include as many of the data elements as possible that CMS needs to complete its analyses."

Vote

Ms. Banks made a motion to approve the recommendation letter (with additional non-substantive refinements related to wordsmithing and formatting), which was seconded by Dr. Mays. Ms. Hines called for a vote of NCVHS Committee members; 10 members voted in favor of approving the letter and thus the letter is approved (with non-substantive changes).

Closing Remarks and Adjourn—Ms. Monson, Chair

Ms. Monson noted that the 2022 Workplan will be discussed in an upcoming Executive Subcommittee meeting. Ms. Monson thanked Subcommittee staff members, invited speakers, the NCVHS team, and the Rose Li and Associates team for their support and adjourned the meeting.

I hereby certify that, to the best of my knowledge, the foregoing summary of minutes is accurate and complete.

Jacki Monson, JD, Chair — October 26, 2022
National Committee on Vital and Health Statistics — Date