Subcommittee on Privacy, Confidentiality, and Security

Meeting Summary

September 14, 2020

National Committee on Vital and Health Statistics (NCVHS)

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

This report was written by NCVHS consultant Rebecca Lazeration, MA, and colleagues at Rose Li and Associates, Inc., in collaboration with NCVHS members and staff.

NCVHS Members and Staff in Attendance

Frank Pasquale, JD, M.Phil., Subcommittee Chair*
William W. Stead, MD, NCVHS Chair
Denise Chrysler, JD*
James (Jim) Cimino, MD
Nick L. Coussoule*
Jamie Ferguson
Melissa M. Goldstein, JD*
Richard W. Landen, MBA, MPH
Vickie M. Mays, PhD, MSPH*
Jacki Monson, JD*
Wu Xu, PhD

*Member of the Subcommittee on Privacy, Confidentiality, and Security

Rachel Seeger, MA, MPA
Lead Staff to the Subcommittee on Privacy, Confidentiality, and Security
Senior Advisor, Public Affairs and Outreach
Office for Civil Rights (OCR), HHS

Maya Bernstein, JD
Staff to the Subcommittee on Privacy, Confidentiality, and Security
Senior Advisor, Privacy Policy
Office of Science and Data Policy
Office of the Assistant Secretary for Planning and Evaluation, HHS

Rebecca Hines, MHS
NCVHS Executive Secretary/Designated Federal Officer
Health Scientist
NCHS, CDC, HHS

Geneva Cashaw
Committee Management Assistant
NCHS, CDC, HHS

Marietta Squire
Committee Management Specialist
NCHS, CDC, HHS

See Appendix B and C for complete lists of meeting participants.

NCVHS—The National Committee on Vital and Health Statistics

NCVHS serves as the advisory committee to the Secretary of Health and Human Services (HHS) on health data, statistics, privacy, national health information policy, and the Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. 242k[k]). The Committee also serves as a forum for interaction with interested private-sector groups on important health data issues. Its membership includes experts in health statistics, electronic interchange of health care information, privacy, confidentiality, and security of electronic information, population-based public health, purchasing or financing health care services, integrated computerized health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services. The HHS Secretary appoints 16 of the 18 committee members to 4-year terms. Two additional members are selected by Congress. The NCVHS website provides additional information at ncvhs.hhs.gov.

Issued October 2020

Table of Contents

Introduction and Overview

The National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality, and Security monitors major developments with regard to health information privacy and security.

On September 14, 2020, the Subcommittee convened a meeting to hear testimony from public health practitioners and other experts from multiple fields about privacy, confidentiality, and security considerations for data collection and use during a Public Health Emergency (PHE), such as the COVID-19 PHE. (See Appendix A for meeting agenda and Appendices B and C for lists of invited speakers and attendees). The meeting was structured to achieve three broad objectives:

- Understand current policies and practices involving data collection and use with respect to privacy and security during the COVID-19 PHE;
- Understand challenges and potential areas in need of clarification in light of these practices, new and emerging technology developments, and new and evolving policy directions; and
- Identify best practices and areas where additional technical assistance or guidance may be useful.

The Subcommittee seeks to translate the knowledge gained during this meeting into recommendations to the NCVHS regarding best practices for data collection and use during PHEs. The NCVHS will use the Subcommittee's input to inform the development and dissemination of a toolkit outlining methods and approaches to responsibly collect, use, protect, store, and share data during a pandemic or long-term nationwide PHE.

Background

Prof. Frank Pasquale, chair of the Subcommittee, provided an overview of the Subcommittee's work, starting in 2015, with the NCVHS Toolkit for Communities Using Health Data Report that set the stage for NCVHS advice on data collection policies. That report, combined with past Subcommittee work in health care data beyond HIPAA, provides the foundation for considering the changing health data landscape. Researchers and policy makers need to consider entities beyond those covered by HIPAA given the impact of Big Data on the ability of anyone who accesses it to make health inferences.

The Subcommittee's determination of the proper scope of data collection, analysis, and sharing during a PHE must balance three concerns that are often in tension. The first concern asserts that rules regarding collection, analysis, use, and data sharing impede effective response. An equal and opposite concern asserts that without robust and enforceable rules the public cannot trust the data systems needed for effective response. A final concern asserts that claims about privacy, confidentiality, and security could be opportunistically raised to block data sharing that could benefit the broader population. The Subcommittee members must balance these concerns when recommending policies and practices to address data safety during a PHE.

While drafting its recommendations, the Subcommittee should consider which fair information principles should apply during a pandemic. Public health professionals need to be able to collect data quickly and efficiently—as illustrated by states and countries that effectively lowered infection and death rates through early identification of infection clusters. For example, Taiwan has reported only 7 deaths in a country of 28 million people, whereas Florida has reported 12,000 deaths in a state of 28 million people. However, the data being collected are exceptionally sensitive because COVID-19 outcomes are not binary, that is, survival or mortality; rather, its effects on people who survive can be long-lasting. Therefore, both the sensitivity and importance of the data must be factored into the identification of fair information principles that should apply during a PHE.

Another set of questions for consideration relate to best practices for properly addressing emergency authorities (such as Notifications of Enforcement Discretion and waivers under Section 1135(b)(7) of the Social Security Act). For example, should each PHE response be unique, or can generalizable principles allow for data liquidity and access while ensuring proper data use? What data should be collected to ensure comprehensive understanding of all dimensions of the PHE without overwhelming health care providers and public health officials? In its recommendations to the NCVHS, the Subcommittee should seek a balance between collecting the data needed for an effective response and establishing reasonable data collection principles.

Finally, Subcommittee members should consider what data collection rules may be overridden to advance public health and what rules must be upheld. The field may determine that some privacy and data rights are inalienable, even during a PHE. On this topic, the Subcommittee should seek a balance between the appropriateness and legality of overriding federal and state privacy laws to obtain the necessary information and the protection of individuals' privacy. Its deliberations should address (1) to what extent are new forms of legislation, regulation, and guidance needed and appropriate; (2) what situations call for identifiable, rather, than aggregate data; and (3) to what level can datasets be deidentified to increase data utility while maintaining patient privacy.

The Subcommittee has much to learn from other countries about the role of health data strategy and public confidence in that strategy in efforts to reduce infection and death rates. Ultimately the Subcommittee seeks to consider the concerns of all stakeholders as it develops recommendations for NCVHS, which will be compiled in a separate document during the weeks following this meeting.

After this stage-setting overview of the meeting purpose and context, three panels of invited experts offered their perspectives to inform the Subcommittee's work, beginning with the topic of "Data Collection and Use."

Data Collection and Use Panel

Ashkan Soltani

Independent Researcher and Technologist

Health care researchers and technologists have made a concerted effort to use data and technology to inform their response to the widespread COVID-19 pandemic. They have relied on digital tools to collect and analyze data for symptom tracking, quarantine detection, and exposure tracking. These experts' strong response was in part a reaction to the lack of coordinated efforts in the United States to respond to the pandemic, although the tools have been used domestically and internationally. However, because of the ad hoc nature of their creation, many of these tools fall outside the definition of covered health agencies or entities protected by HIPAA.

For example, smartphone applications to support contact tracing, through self-report and automatic data retrieval, and exposure notification are not covered by health care data protections. Used in Singapore, South Korea, Australia, and the United Kingdom with mixed results, these apps allow users to self-report infection to health agencies, which in turn use location data to identify and notify other users who may have been in contact with an infected individual. One major barrier to uptake of the technology has been user concern about the collection of their location and contact information by nongovernment entities. Consequently, Google and Apple were tasked with gatekeeping all applications developed on their platforms globally and with addressing barriers to development of these new apps, such as technical limitations of background Bluetooth technology to accurately identify contacts. In response, Google and Apple promoted the contact tracing application programming interface (API)—later called the exposure notification API—that attempted to perform the same function in an anonymized way. The API allows for users to opt-in to using built-in tools to send pseudonymous identifiers to record contacts with other users through deidentified information. Users can notify the system of positive viral status, which then traces contacts and sends automated alerts to individuals who may have been exposed. The API circumvents notification of contact to central authorities.

This approach poses its own set of privacy and accuracy concerns. Adoption of a system is voluntary, which means that not all smartphone users are connected to the location tracking. Response to a notification of contact with an infected individual is also voluntary. Researchers and technology experts do not know whether individuals will act on an exposure notification if no authority confirms the accuracy of the notification or provides guidance on next steps. Mr. Soltani added that they also do not know whether individuals will voluntarily isolate, given the current social environment within the United States in which many individuals will not comply with mask-wearing requirements.

Experts are also unsure about the technology's efficacy as a standalone tool to accurately perform contact tracing and exposure reporting. Bluetooth contact tracing is based on proximity, and therefore may inaccurately report individuals on different floors of buildings as having been in contact. Further, given the incomplete coverage of the

system, a lack of reports does not mean that an individual has not been in contact with an infected individual. Even if smartphone penetration were 100 percent in the United States, the apps would provide at best a 64 percent detection rate—potentially providing individuals with a false sense of security when navigating their community.

Another concern relates to the platform's security. The developers have ensured that no central authority can monitor contacts; however, as with any smartphone app, the platform is vulnerable to re-identification. A hacker could set up a Bluetooth detector in conjunction with a camera to identify individuals who visit specified locations. Hackers could also shut down or flood the network in a given area to interrupt the service and provide potential false negatives. In recent work, Mr. Soltani found ways that hackers could create false alerts of either contact or exposure. Such an attack could be targeted around key areas or events such as an election to cause panic.

The API system has weaknesses in part because Google and Apple acted almost unilaterally to develop it. These companies and researchers and technology experts are making decisions that involve large trade-offs between privacy, security, and efficacy independent of policy leaders. Although health agencies and administrations are now creating their own tracking applications, they will likely find it difficult to convince the public to widely adopt tools beyond those already available.

Allison Arwady, MD MPH

Chicago Department of Public Health

Public health agencies and departments, such as the Chicago Department of Public Health, are responsible for translating data collected during the pandemic into response plans. In Chicago, the Department of Public Health is also responsible for distributing testing resources, providing additional outreach, and connecting people with health care. The COVID-19 pandemic has made privacy a mainstream issue at the local and state levels. Even before the pandemic, health departments needed identifiable data to make progress toward fighting HIV infection, lead poisoning, and communicable diseases.

In countries with national health care systems, health care providers have access to the data needed to track the course of their patients' care. In the decentralized U.S. health care system, public health departments are often forced to pull together data from public health silos and health care silos to create a patchwork picture of their residents' health. In addition, technology is outpacing health care practices and privacy protection policies -- a challenge that the pandemic has brought to the fore -- and is forcing departments to quickly modernize public health systems.

State and federal law have failed to keep pace with public health practice. Therefore, local public health agencies must ensure that privacy and security are embedded in their policies and practices—even beyond what is required by HIPAA. Further, public health officials must ask not only whether data *can* be shared, but whether data *should* be shared. All of the rules and regulations can make it difficult for the public to understand how their individual rights are being protected while officials work to improve overall public health.

Public health officials and health care providers must consider the pandemic response in the broader domain of public health laws and their evolution. For example, in Chicago, technology has enabled tracking of HIV-positive individuals in the health care system so that, if an individual who has lapsed in care arrives in an emergency department, the health care workers are aware of the patient's status and can reinstate a regular care schedule. This balancing act of sharing information for critical health concerns (e.g., HIV, lead poisoning) is where health care and public health divide. Although health care considers the privacy of the individual, the public health domain must consider the greater good—which sometimes outweighs the rights of individuals (e.g., required reporting laws for child abuse or communicable diseases). The COVID-19 pandemic has brought these issues to the forefront of the public's mind and has reminded public health departments of the importance of modernizing systems to meet evolving health care needs and technological advancements.

Robert Grossman, PhD

University of Chicago

The Rockefeller Foundation advocated for national COVID-19 testing and tracing that would (1) grow testing to 30 million tests per week, (2) launch a COVID-19 Community Healthcare Corps for testing and contact tracing, and (3) create a COVID-19 data commons and digital platform. The third activity must balance data privacy and security with data utility; however, if data are not collected in a centralized platform, then public health professionals cannot maximize the use of the data produced by the approximately 5.3 million tests that are currently performed each week.

In response to the pandemic, many traditional and nontraditional groups and organizations have started to collect various forms of COVID-19-related data—including incidence and count data, clinical and imaging data, viral sequence data, and mobility and behavior data. Widespread sharing of information about the SARS-CoV-2 virus has facilitated global progress toward developing vaccine progress. This fast progress illustrates the potential for a large, open, data-sharing platform to support PHE responses.

Researchers must consider data privacy and security when developing such a platform. They must make decisions about aggregation or disaggregation of data and frequency of data collection (e.g., once per day or continuous). Each decision will have different security and privacy implications but can be made in a way that minimizes the risk to the public while maximizing the possible analyses that can be performed with the data collected. Most importantly, the large technology providers (e.g., Apple, Google) are providing public health data tools at scales never available before. These companies also offer cloud platforms that simplify data analysis and application of predictive learning models, as well as provide built-in security measures.

Data-driven decision making during a PHE can be separated into the following silos: public health, patient care and hospital practice, medical research, data to support governance, and data to improve community life. These last two silos are often overlooked. All five silos ensure that communities have the data needed to make local-level decisions about PHE response (e.g., incidence levels and trends). A large database to track the data in the last three silos would complement the data collected in the first two silos. To create such a database, researchers may wish to implement a data commons.

Data commonses are software platforms that combine data collection, cloud-based computing infrastructure, and commonly used tools and services to create a resource for securely managing, analyzing, integrating, and sharing data with a community while protecting privacy. Data commonses can balance patient data protections with open research that benefits patients. The National Institutes of Health (NIH) has created multiple data commonses that illustrate their benefits to the larger research community in the everyday and PHE settings.

A public-private partnership is developing and operating the Pandemic Response Commons to support state, regional, and local groups during the COVID-19 PHE and future PHEs. The Commons can create smaller commonses in an infrastructure designed to track and evaluate pandemics and epidemics that provides users with legal templates, open source software, and other tools. A Commons has already been created for the Chicago region through a public-private partnership funded by philanthropy and in-kind donations, which serves as a model for others to follow suit.

Dr. Grossman presented several recommendations for future actions: (1) establish national and regional commonses to support PHEs, (2) create trust relationships between data commonses to allow for sharing data and federating queries, (3) create a persistent data commons infrastructure to respond to future epidemics and pandemics, and (4) funders should require researchers to share data and provide a computing infrastructure to allow the community to work together in response to future PHEs.

At the conclusion of the presentations, Prof. Frank Pasquale, Subcommittee Chair, opened up the session for questions and dialogue between NCVHS members and the invited experts.

Discussion

Risk of Manipulation of Technology

The Decentralized Privacy-Preserving Proximity Tracing (DP3T) API—an inspiration for the Google/Apple API—has a security document that outlines the risks of manipulation, hacking, or other forms of interference with the system. The National Cyber Security Centre performed a security analysis of this decentralized API and identified manipulation risks similar to those for the centralized API. Mr. Soltani noted that tradeoffs exist between the centralized and decentralized approaches. A centralized system offers fewer privacy protections, and its manipulation could have a wider impact; however, the system can be better protected. A decentralized system offers greater privacy protections, but identifying a hack of the system can be difficult without privacy invasive telemetry. Mr. Soltani emphasized that the lack of input from privacy-concerned organizations such as the Subcommittee during development of the Google/Apple API have led to his concerns about the apps' balance between usability and privacy. Responsibility for platform security rests with the implementing health agencies.

Long-Term Privacy Needs

Individuals infected with COVID-19 will feel its effects for a long time. Some tools have integrated explicit consent documents for the use of privacy-preserved data in the long term. For example, aggregated statistical data collected from tracking applications can be used over the long term without risking the privacy of individual users. When explicit consent is minimal -- for example, the data received by the Chicago Department of Public Health -- the appropriate institutional review boards (IRBs) must determine whether the questions being asked of the data align with public health needs. Any procedures that require sample collection or additional interviews will require additional consent of the individual or oversight from the IRB. For example, a case control study of an outbreak location would require further consent at the individual level. Another example used de-aggregated data to study differences between races and ethnicities, which required IRB approval to ensure that the data were used for appropriate public health reasons.

National Identification

HIPAA legislation called for the development of a national patient identifier system that would assign each person in the United States a unique identifier to be used across the health care spectrum. Citing privacy concerns, Congress banned funding for such a system. The lack of such an identifier complicates harmonization of data across databases and silos. However, a larger issue can be the requirements about which data can be shared from each silo and with whom. For example, it took the Chicago Department of Public Health a long time to match children with lead poisoning with participants in the housing choice voucher program because of restrictions on data sharing across platforms.

When able to make connections, the Chicago Department of Public Health has partnered with clinical and technological entities to assist with the behind-the-scenes needs of their public health projects. These partnerships are first and foremost focused on protecting the privacy of Chicago's citizens. Dr. Grossman noted that current technology can link records using cryptographic short-term identifiers, which could help to maintain privacy while data remains siloed. He added that policy issues may prevent this work, but such opportunities may warrant exploration by the Subcommittee and the Department of Health and Human Services.

Data Commons

Many of the current data laws are outdated and will be obsolete and perhaps destructively limiting in a post-COVID-19 data environment. Technology has made great strides, enabling local public health agencies to create daily reports of COVID-19 activity, which the public is accessing in numbers not previously recorded for local public health reports. This access to open, transparent data is setting a new standard for the public, and annual reports on other pressing health issues may not be sufficient in a post-COVID environment. However, outdated laws limit the vital statistics that local public health agencies can share. States need to push for legislation and policies that

allow such agencies to access data that should be reported as part of their responses to PHEs and other critical health concerns (e.g., communicable disease).

A data commons could provide the modern technical structure needed to support public health and other health care needs. Each data silo will always require its own data type to accomplish its task (e.g., contact data for public health silo). Current structures are not easy to adapt to PHEs. A data commons can bridge silos through a consistent platform that can be leveraged by all users and can address pressing and sudden health needs.

Contact Tracing and Exposure Notification Applications

Prof. Pasquale asked each panelist to summarize his/her opinions of exposure notification or contact tracing apps on mobile devices. Mr. Soltani said that the apps' success will depend on guidance from public health officials about their use and effectiveness. Mr. Soltani expressed concern about insufficient understanding of the apps' underlying mechanisms and about blind faith acceptance that the apps can accurately track outbreaks and clusters.

Commissioner Arwady noted that a primary focus of local health departments is maintaining the public's trust, which has become increasingly difficult in a politicized environment that is inundated by misinformation. The public has misconstrued public health agencies' use of anonymized cell phone data to track stay-at-home compliance and similar measures as "the government is tracking me." In her role as Commissioner, she has met individuals who believe that COVID-19 vaccination is a government conspiracy to implant tracking chips in the public. She is enthusiastic about these apps' potential but acknowledges concerns about overstepping boundaries in terms of privacy.

Dr. Grossman noted that contact tracing apps do not fit within the currently defined health care data silos, and therefore there are limitations on the data collected by these applications. He added that mistrust of these apps has caused his team to focus on other technologies. However, confusion and lack of trust could be reduced through community engagement and discouragement of specified tracing (e.g., based on race/ethnicity).

Technology and Ethics Panel

Four invited experts provided testimony on technology and ethics.

Danielle Allen, PhD

Harvard University

PHE technology can be understood as either testing technology or digital technology (e.g., exposure and notification tools). Both forms of technology pose challenges because they do not fit into the existing structure for addressing societal health, that is, something is a matter of health care or of public health surveillance. Many current activities fall within both of these categories and create spaces in need of rules and regulations to govern implementation tools. For example, colleges and universities have started routine testing of asymptomatic individuals. A related example is exposure notification tools in use in other countries. Both forms of technology present new ways of interacting with the health care system, that do not fall neatly within the HIPAA framework, and create "category confusion."

The Centers for Disease Control and Prevention (CDC) uses three categories for testing: diagnostic, screening, and surveillance. In contrast, HHS uses two categories: diagnostic and surveillance. CDC's screening category is relatively new, with unstable vocabulary in use, but generally refers to testing of asymptomatic individuals without known or suspected exposure with tests typically completed in a Clinical Laboratory Improvement Amendments (CLIA) lab following Food and Drug Administration (FDA) policies. The emergence of screening for infectious diseases has introduced less expensive tests, which can be used outside the laboratory setting, but this broad health screening is not captured in the existing body of policies and regulations for health systems. In addition, CLIA labs are unable to handle the volume of testing that is needed for the pandemic, which raises privacy concerns because non-CLIA labs may not be beholden to HIPAA compliance. While screening of asymptomatic

individuals falls under screening testing within HIPAA guidelines, the laboratories completing the testing (e.g., universities) may not always be HIPAA-covered entities.

As a result, policy makers and health care workers need clarification about HIPAA's application to screening testing sites for PHEs. This clarification may require a broadened list of HIPAA-covered entities. Broadening the definition would bring the majority of COVID-19 testing under HIPAA protection, which already contains the framework required for balancing the protection of the individual rights and public needs. Relatedly, health care workers need clarified norms to know when screening should be confirmed with diagnostic testing—which is well-integrated into public health systems. The absence of such norms affects how data are integrated into health systems. The system also requires clarification about how payment systems will cover, or whether they will cover, screening testing because this category falls between health care costs and public health funding.

Drawing on a white paper from a rapid response series on digital tools for COVID-19 contact tracing, Dr. Allen noted that contact tracing and notification apps using Bluetooth that have been taken up in many European countries contrast with screening testing and are not occurring within health care facilities. The information about potential exposure provided by these apps is not a direct assessment of health care service and therefore not covered by HIPAA privacy protections. Therefore, public health workers require an alternative form of protections. The authors suggest that federal legislation must provide safeguards and hold governments and companies accountable for individuals' privacy, and therefore the federal government should provide resources to the Federal Trade Commission (FTC) and state agencies to hold companies accountable for privacy violations or deceptive practices. The authors outlined the following principles for this legislation: meaningful consent, transparency, data minimization, limited retention period, prohibition of secondary uses, data security, and equity.

John W. Loonsk, MD

Johns Hopkins University

Electronic case reporting (eCR) -- a joint initiative of the Council of State and Territorial Epidemiologists, CDC, and the Association of Public Health Laboratories -- is the automated identification of reportable health events in electronic health records and their transmission to state and local public health authorities for review and action. COVID-19 has made clear the need for essential clinical data for outbreak management at public health agencies, which could be met by eCR. Since the identification of COVID-19 as a PHE, the eCR Now initiative has worked to initiate eCR reporting at more than 4,800 sites.

Dr. Loonsk stated that case reporting laws exist in all states, and, with the support of HIPAA, necessary identifiable data are required to be reported to public health agencies with or without patient consent. The Electronic Initial Case Report (EICR) standards denote what data are appropriate for reporting in a case report—although the current focus is on reporting COVID-19-related data. eCR is in process but has not been effectively advanced by federal regulations and is only a choice in Medicare and Medicaid's Promoting Interoperability toolkit. The initiation of eCR would remove the requirement for manual reporting and would reduce the burden on health care workers to report the critical public health data.

Over the course of the COVID-19 pandemic, public health professionals and policy makers recognized that public health agencies may need broader authority to collect data. The eCR data could fill this gap. However, some dissenters have expressed that the Continuity of Care Document should be sufficient, even though it does not contain the data that some public health officials need and contains some clinical data that these officials are not authorized to access nor do they want to collect it. These dissenting perspectives in part illustrate how existing public health requirements and authorities have been inadequately advanced in the age of advancing technologies.

Dr. Loonsk illustrated how the Trusted Exchange Framework and Common Agreement (TEFCA) and health information networks can help meet the needs of public health agencies. Careful attention should be paid to how these networks will be validated from both the data access and privacy policy standpoints while ensuring that the necessary public health agencies receive the data they need to make informed decisions.

Kate Goodin, MS, MPH

Tennessee Department of Health; Council of State and Territorial Epidemiologists

Decisions made about public health data during the COVID-19 pandemic will have a lasting effect on the potential for public health agencies to respond to future PHEs. Small versions of such responses occur frequently (e.g., salmonella outbreak, fungal meningitis outbreak), with each event requiring different types of data for tracking and prevention. Often foodborne illnesses draw more public interest than smaller outbreaks because the public wants to know what steps to take to prevent foodborne illness. However, some PHEs lead to stigmatization of ethnic groups or individuals who traveled to certain areas (e.g., Ebola infection) and privacy protections, and therefore consideration of what information should be shared and what remains private becomes more important.

Many individuals and businesses are not aware that public health agencies are authorized to collect identifiable clinical information as necessary to control diseases in the community. These disclosures are authorized through overarching rules that define the public health authority and provide guidance on how the data can be received and stored. Most public health agencies are further defined by state and local rules and regulations, with each state maintaining a statute that compels the reporting of specified conditions, the content of the reports, the method of reporting, and the authority to access medical records to compile these reports. HIPAA can also apply to local agencies in different ways, with public health entities classified as covered, hybrid, or exempt. These classifications have a large impact on what information can be collected and shared by those entities. These differing rules make HIPAA penalties for unauthorize disclosures of information difficult to track and discern, requiring agencies to handle matters on a case-by-case basis.

Public health agencies exist within a set of ethical principles that govern actions beyond the letter of law and statutes that have been heavily influenced by the history of medical practice in the United States. For data collection and sharing, these ethical principles address whether data elements are essential for collection, how analyses will change based on the information collected, and how an analysis change will influence the goals of the agency to protect public health. Agencies must also consider whether data collection translates to actions and what impacts on individuals and the community these actions might have. Finally, agencies must maintain the trust of the public for both collection and disclosure of data, which sometimes runs counter to the trust of other institutions. For example, using incomplete data during a foodborne illness outbreak may harm a business but withholding the information may cause more individuals to become sick.

Ms. Goodin presented one potential health information exchange flow. She noted that often these diagrams fail to account for public health agencies or their role as an endpoint for information flow. These perspectives ignore the role that public health agencies play in the health care continuum. Public health needs to be considered more often during discussions about information exchange in health care. The exchange should be two way—that is, the public health agency receives the information it needs, and the agency shares information with other agencies or health care providers. For example, Ms. Goodin displayed a redacted COVID-19 test report that was shared with a public health agency. She noted the lack of information received by the agency, including identifiable information, where the test was performed, and what type of test was performed. These low-readability, low-information reports pre-date the COVID-19 pandemic but illustrate the critical need for better information sharing.

Ms. Goodin also presented a list of groups that have requested identifiable case-based COVID-19 data. Often state agencies could not, and should not, comply with the requests. This list also illustrates the need for policies and regulations that denote who can request data, and under what circumstances, and what information should be shared to balance privacy with public need.

Stacey Mondschein Katz, Esq.

Maine Department of Health and Human Services

The Maine Department of Health and Human Services (the Department) is a hybrid-covered entity for HIPAA, which means that parts of the department are covered by HIPAA (MaineCare and Maine CDC's [MeCDC] Health and Environmental Testing Laboratory) and other parts are considered a Public Health Authority and are not covered by HIPAA (other MeCDC programs). The Department's strong privacy framework seeks to protect

identifiable consumer data, with privacy and security liaisons in each office. The MeCDC also maintains its own additional policies and processes for responding to requests for data, which requires that requests undergo the Department's research process to ensure confidentiality and tracking of the data flow, as well as review by the IRB and HIPAA Privacy Board as applicable.

Per these regulations, COVID-19 laboratory results are kept secure in an electronic system with administrative, physical, and technical safeguards. Results from COVID-19 testing are part of an individual's medical record and therefore subject to protection by state and federal confidentiality laws, including HIPAA. However, when the results are reported by providers to the Disease Surveillance program -- part of MeCDC -- HIPAA no longer applies, and information is protected instead by state law.

Patient test results are merged into the National Electronic Disease Surveillance System (NEDSS), where data are reviewed to identify confirmed cases. Investigators track and enter close contacts into NEDSS as well. These close contacts are transferred from NEDSS to the Sara Alert™ system, through which they are contacted via phone and, with permission, enrolled into the contract tracing texting program. This allows for case investigators or contact tracers to identify individuals in quarantine with social services needs and to connect these individuals with the Department's Commissioner's office or contracted agencies to fill those needs.

Deidentified information for COVID-19 testing is also shared with the MeCDC dashboard (e.g., cases by county, cases by zip code), news media (e.g., press briefings), case investigations, and public health activities (e.g., surveillance, containment, analysis). Information is deidentified per HIPAA best practices. Data are updated weekly to ensure that individuals' privacy in smaller communities is protected. All access to the COVID-19 electronic systems is audited for appropriateness. Case investigators and contact tracers receive confidentiality training, and contract staff sign confidentiality agreements. Any privacy or security concerns are reported to the supervisor and a MeCDC Privacy/Security Liaison.

One of the biggest risks in the system is human error—particularly with the evolving office situation of working from home part-time or full-time, where family members may have access to work platforms. Users of sensitive data must be particularly careful to ensure appropriate safeguards to information, be regularly educated to maintain awareness, and have processes in place to mitigate incidences (e.g., information leaks, phishing scams).

Should consumer-identifiable information be required, the MeCDC requires a Data Sharing and Protection Agreement that includes consumer confidentiality, agreement not to contact individuals, agreement to contact the Department within 24 hours in the event of a breach, and a promise to work cooperatively with the Department on any investigations.

The MeCDC has received limited access to statewide information exchange platforms during the pandemic to assist with containment and care. This access allows providers to view patient records, including COVID-19 test status. It also permits MeCDC and some contracted staff to access patient health information within PHE rules. Access to these records is closely audited and monitored, and concerns are communicated with the Department's Director of Healthcare Privacy. Finally, the state's rule on responding to a public health emergency, such as the one currently declared by the Governor, permits flexibility. The state may take the steps necessary to contain or lessen the outbreak, depending upon the situation.

Discussion

Applicability of Daily Practice to PHEs

Ms. Allen clarified that the policies discussed during her presentation are applicable in both a PHE and general setting. She added that the volume of screening testing dictates integration into HIPAA-compliant protocols. The core needs during PHEs are for existing structures and organizations to adjust.

Ms. Goodin agreed that the issues discussed during her presentation are day-to-day but have been exacerbated by the PHE. The PHE has forced local and state agencies to consider whether the balance between privacy and public health needs to shift. The scale of a given PHE determines how quickly decisions about balance need to be made.

From this perspective, the adoption of ELR and eCR is important because these mechanisms are easier to scale up in larger PHEs.

Dr. Loonsk added that an ongoing policy discussion is the importance of dual use—policies should accommodate routine activities and emergency activities to eliminate the need to implement new technologies and policies during a PHE. This dual use principle should be applied to all technologies, including the new mobile apps.

Ms. Katz added that departments and entities need to be able to leverage small or independent response initiatives during large-scale PHEs to quarantine and contain the outbreak, and the standard for containment and quarantine may differ between incidents. The policies should be flexible to allow for these changes.

Modernization Efforts

Dr. Loonsk mentioned that CDC is working on data modernization efforts that may include funding for updating practices. During this work, infrastructure will be adjusted to improve response to future PHEs. However, sustained funding is needed to ensure that public health efforts, especially those related to public health technologies, can be implemented *and* maintained. Sustained funding for public health has dwindled over the past decade. Ms. Goodin agreed, noting that the COVID-19 outbreak occurred when funds for data modernization were being distributed, which has necessarily diverted the field's focus. However, data modernization cannot occur unless the necessary level of technology is available, and efforts are made to harmonize communications with public health.

Aligning Healthcare Categories

To tackle the disparate handling of COVID-19 testing for screening, Dr. Allen recommend that CDC and HHS align their vocabulary and health care categories. The pandemic is unique because testing results are not typically returned to the individual tested. Therefore, this testing does not meet the definition of surveillance, despite being a critical public health function. Once categories and their definitions are finalized, the field should set standards for these types of screening to ensure that the public's privacy is protected and that results are reliable. In the meantime, to provide the necessary protections to the unique testing facilities, Dr. Allen recommended that the definition of HIPAA-covered entities be expanded.

Targeting Populations

Ms. Goodin stated that the lack of data received by public health authorities during the COVID-19 pandemic has limited disclosures to targeted populations. For example, the Tennessee Department of Health is not receiving gender or race/ethnicity data in the volume needed to identify at-risk minorities. She added that her department has faced translation of information issues. For example, misunderstanding of annotations of data has led to multiple edits and explanations of datasets, increasing work for the department and slowing disclosure of additional information.

State of Privacy Policy

Ms. Goodin clarified that no single law or regulation creates issues for local and state public health agencies; rather, the patchwork of rules and laws across state and local jurisdictions may conflict with federal laws and complicate implementation of national standards. Another challenge relates to education laws, which are largely dictated by state and local education agencies—that is, public health workers are prevented from responding to situations where children are affected in a school environment by a communicable disease because of schools' concerns about disclosure.

Bias and Discrimination

Bryant Thomas Karras, MD

Office of the State Health Officer, Washington State

Contact tracing is not a new process; it has been applied in responses to numerous communicable diseases and other health concerns and therefore is common practice in the public health field. To regain public trust in the

process, the field must emphasize the intent of contact tracing, which is not to collect social security numbers, immigration status, socioeconomic status, or marital status.

Washington State was the location of the first confirmed U.S. case of COVID-19. Since the early days of the pandemic, the state has worked to connect numerous new technologies (e.g., Sara Alert) to the existing Washington Disease Reporting System to create a multi-directional information flow among multiple systems inside and outside the agency to improve interoperability. This new system of systems required a workforce with expertise to manage its complexities to benefit the end user. Major challenges related to the need for a patient identifier to ease harmonization across platforms, for extensible cloud-based capacities, for integration of multiple data sources, and to protect privacy during public reporting and disclosure requests. Dr. Karras previewed one outcome of this effort—a data dashboard that can dynamically present COVID-19 data throughout the state. The data are updated daily, which allows the users to track the progression of the pandemic.

The new system enveloped multiple innovations that require integration and resources. Dr. Karras highlighted the Google/Apple API described by Mr. Soltani. This technology seeks to meet a major need, which is to provide contact tracing in a crowded city to accurately ping people who have come into contact with an infected person, particularly among those not abiding by social distancing or mask wearing rules. The API app was piloted at the University of Washington, and its uptake may have been hindered by misinformation spread by the press, but it remains one of the most promising advancements in contact tracing in recent decades.

The need to strike a balance between public health and the privacy of the individual is paramount. Important privacy-related considerations for public health surveillance include the following: (1) privacy and confidentiality are the cornerstones of public health collection; (2) HIPAA does not limit protected health information provided to public health agencies, but state laws do; and (3) identifiable patient data are exempt from disclosure under state rules and codes.

Finally, centralizing data with CDC or HHS does not negate states' responsibility to ensure privacy and confidentiality. Many systems have insufficient funding to modernize to new standards, and interoperability between states is greatly limited. Many new systems are promising, but HHS must work to ensure their full development and incorporation within state and local agencies.

Mary L. Gray, PhD

Microsoft Research

The COVID-19 pandemic has presented the opportunity for public health departments to partner with communities in a way that is critical to rebuild public health relationships that can endure in the aftermath of the pandemic. This opportunity requires public health groups to prove that their methods to ensure security and privacy are strong and serve the public's best interest. However, many of the security and privacy techniques to deidentify data are limited, meaning that public-private partnerships that collect data cannot be the data stewards that the public needs. The field suffers from an overreliance on deidentification practices, and the subsequent false security of data trafficking without public buy-in will only serve to further erode public trust.

In addition, public health workers must recognize that they cannot guarantee people's privacy. Because they cannot assure privacy, public health systems must build strong relationships of trust with the communities that are being disproportionately impacted by COVID-19. To date, technological solutions have focused on individual privacy and security, ignoring the need to build trust through the technologies.

Further, government agencies need to understand the limits to deidentifying public health surveillance data and to generating meaningful data from anonymous self-reporting via tracking technologies. The countries that achieved success with these technologies had robust trust in government infrastructure, which is lacking in the United States. Based on preliminary studies, Dr. Gray advocates for public health departments to deputize key community groups who can serve among the higher-risk communities as liaisons.

Computer scientists understand that 87 percent of the United States population can be identified by accessing a small number of identifiers, with half the population likely to be identified by place, gender, and date of birth. This

information can be bought on the internet. Therefore, the problem is not the dataset collected, but that the data can be enhanced with other datasets to easily identify individuals. This lack of security explains why the 2020 Census switched to differential privacy to protect respondent-level data. So, while the capacity for using data has advanced, the mechanisms for engaging the public and receiving consent and buy-in are failing. Public health agencies are contributing to this problem by collecting data without an awareness of what limits and vulnerabilities are being introduced.

Current applications that perform contact tracing do not build relationships with individuals who may become infected later and at that time may require more assistance from the public health agency. Frontline contact tracers can fill the need of aiding individuals by identifying individuals at community's margins (e.g., the elderly) who are most in need of assistance. These contact tracers can help stop the spread of COVID-19 by allowing communities and health care workers to quickly gather and disseminate resources, not just identify who has been exposed.

Contact tracing is the proven standard for managing the spread of life-threatening infectious diseases. It relies on meticulous data collection. Further, because a text notification about exposure is likely insufficient to garner a response, it requires the deployment of trained counselors to connect to the communities that they serve. The magnitude of the labor force needed to complete contact tracing during the COVID-19 pandemic is daunting, only because public health workers are focusing on a large rollout rather than the small clusters of outbreaks in the hardest hit communities.

In addition, technology-based tracing is fraught with issues, often missing data from infected people who are not carrying their phones or missing people who lack smartphone access. Most importantly, the technology will lead to inaccurate reporting of contacts. Definitions of high-risk exposure are not yet clearly defined and therefore cannot be accurately reported. The false positives and false negatives likely generated by smartphone contact tracing apps will create more problems than they will solve. To be successful, trained health care workers should analyze the data to assess the risk associated with each interaction, and the toolkits they use to do so should be improved.

Most problematic is the treatment of technology as a solution to the real issue, which is that the most vulnerable people (e.g., undocumented workers) will likely misrepresent their locations, activities, and contacts if they are uncomfortable with, or mistrust, the individual with whom they are interacting. As such, contact tracing hinges on deeply human interactions that are about trust. Requiring use of an app in a workplace is a coercive tactic, which would not be allowed in a research setting. A narrow focus on smartphone apps will distract public health workers from rolling out comprehensive contact tracing strategies with mechanisms to hold data in trust.

Dr. Gray highlighted the need for technology that enables: (1) dynamic electronic reference tools that provide well-indexed answers to people's questions in their first language; (2) methods for public health workers to track people in quarantine and to provide them with the resources they may need (e.g., groceries), which will require an information-sharing vs. privacy-first approach; and (3) secure, centralized data storage that ensures local-level community data trusts. However, glamorizing technology as a replacement for health care workers is a dangerous distraction. Health care workers are the key to successful contact tracing and other public health efforts.

Sean Martin McDonald, JD, MA

Centre for International Governance Innovation

Mr. McDonald noted that he has worked with digital contact tracing since the Ebola outbreak in 2015, which showed that movement tracking is an inadequate proxy for disease tracking and is also illegal. The COVID-19 pandemic has revealed biases in deploying public technology, which underscores the need for intervention at the top of the funnel (i.e., laws and regulations that govern launch of health-adjacent products). Legislators and policy makers need to consider the role of medical regulators in the validation process and the communication of that process to the public.

When publications describe the success of contact tracing applications, they are likely referring to the uptake of the applications. Among the applications in use, the largest number of uptakes was in the hundreds, among a

population of millions. Therefore, the applications have not illustrated fidelity of the notification systems. Contact tracing must be fundamentally connected to care in a way that the contact tracing applications fail to do.

At a fundamental level, there is a problem in evaluating the underlying science before the technology is deployed. Researchers are concentrating on whether a technology can be deployed at a large scale, rather than whether it adds value. And they neglect to understand that millions of smartphones cannot use the apps developed—either due to outdated technology or platform differences (i.e., Google vs. Apple product). The exclusion of many people leads to questions about the technology's credibility and equitability.

Mr. McDonald described the case of Los Angeles, which decided to repurpose a criminal tracing application that was previously determined to be so invasive that it was removed from apps stores. This repurposing (1) removed the possibility of "good faith" trust in the application and (2) failed to protect the integrity of public health and contact tracing. Repurposed tracing applications such as this one have led to an array of politicized reactions to tracing tools. Furthermore, bugs and architectural issues with the technology are resulting in false positives, which are particularly damaging for individuals who may not be able to abide by the quarantine orders without social support.

Mr. McDonald presented the findings of a trust barometer—illustrating changes in public trust from 2019 to 2020. The changes between years showed a decrease in public trust of technology, particularly influenced by the way industries adopt technology. This illustrates that politics influences the communication and rollout of new technologies, and distrust of these rollouts is the root cause of people not adopting new technologies. These trust issues are further complicated by second-order consent, by which employers or local law enforcement require adoption of a specific technology.

Most people experience digital rights through terms of service agreements, which they typically ignore. When a public health response takes the form of a product (e.g., contact tracing application) with a conglomerate (e.g., Google/Apple) instead of a point of contact (e.g., a public health department) communication of issues and concerns from the public become difficult. This chain of command is typically not allowed in the public health sector. The distance between what people are being told and the support they need to follow instructions is leading to a lack of legitimacy and is challenging how institutions engage with the public. When researchers discuss the potential of technology, they must also acknowledge that its current form is delegitimizing the industries it encounters.

Mr. McDonald raised the issue of the Belmont report and the lack of discussion regarding the Common Rule. Public health technology deployments are ignoring the guidelines and validation checks that should be required of such experimental approaches. The implications of government using its emergency power to participate in science infrastructure must be considered. Politics sometimes trumps the rights of the vulnerable. Therefore, when the government is exercising its powers for the public good, public health professionals need to consider how protections that are normally placed on emergency powers can be applied.

Science is dialogical, and during an emergency scientists and researchers need a mechanism to share their concerns and discuss what is in the public's best interest. One such mechanism is a data trust—a tool to build legally enforceable digital governance and rights. Data trusts are based in equity law but implemented in property law. A grantor puts an asset (e.g., data) into a trust, which gives control of the asset to a trustee for a purpose, on behalf of a beneficiary. A data trust is a tool to architect accountability that allows experimentation with the governance and practice that might remediate the existing trust issues.

While these structures exist, researchers must cope with the political nature in which data is architected. Mr. McDonald presented a slide of conclusions and recommendations. He stressed that although privacy, confidentiality, and security are the focuses of the Committee, these concepts in a public health response to a PHE are holistic. He noted that it is worth thinking about the degree of remediation and redress required to address issues such as unvalidated products advanced at a governmental scale. When considering privacy, confidentiality, and security, Mr. McDonald asked the Committee to consider the ways in which actors and actions are needed to create public health responses.

C. Jason Wang, MD, PhD

Center for Policy, Outcomes and Prevention, Stanford University

Taiwan has a population of approximately 24 million, with 1 million individuals commuting to China to work, meaning that the COVID-19 outbreak in China had the potential to quickly affect the population of Taiwan. Taiwan has experience with outbreaks in its population because it was affected by the SARS outbreak in 2003, at which time 346 individuals were infected and 73 people died. Many people who were quarantined ran away because they believed they were being incarcerated, and since that time changes have been made to the Communicable Disease Control Act. These changes relate to the government's ability to stockpile protective equipment in hospitals; the government's ability to regulate gatherings, traffic, evacuation, and other disease control measures; and added penalties for violating quarantine, hoarding resources, or spreading false information. During a pandemic or epidemic, the government can also requisition resources to produce protective equipment. These special powers expire 1 year after an emergency is declared. Different government agencies provide data to the Central Epidemic Command Center (CECC) to perform real-time tracking of an outbreak.

On December 31, 2019, the World Health Organizations was notified of a cluster of cases of COVID-19 in Wuhan, China, and Taiwan officials inspected passengers for symptoms on a direct flight arriving from Wuhan. On January 20, 2020, the CECC was activated, and on January 21 the National Security Council convened to coordinate response efforts. Since that time, anyone entering Taiwan must go through quarantine process, including filling out an online declaration form prior to travel to note symptoms, country of origin, and countries visited in the past 14 days. Passengers arriving from a high-risk country are immediately placed in strict quarantine. Other passengers can quarantine from home after arrival. In the interest of tracking the outbreak, Taiwan linked the National Health Insurance Database with the Customs and Immigration Database, so doctors and nurses are alerted about the patient's travel patterns before a patient visit. In addition, individuals arriving from abroad are not permitted to see a doctor within 14 days of arrival without going through the health department.

Digital epidemiology played a large part in Taiwan's management of the pandemic. This allowed for fast tracking of the core public health functions of case detection, contact tracing, and isolation and quarantine. Technologies such as disease modeling and forecasting using machine learning; large datasets for case identification; electronic monitoring of quarantined individuals; and enhanced contact tracing were all implemented. Some of these methods were controversial, such as the use of Alipay to track and label individuals with a risk code based on their travel habits. Other efforts were plagued by ineffective technologies, such as cheap cellphones causing issues in tracking individuals under quarantine.

In Taiwan, as with all democracies, engendering trust and participation was an important factor—which is why the government had to consider the ethics of using the available data and under what circumstances use of data was ethically justifiable. This included the privacy concerns over tracking cellphone location—which is normally not used except by law enforcement to track and impose consequences on individuals. Relatedly, autonomy, or removal of the requirement for informed consent for use of personal information, was raised as an ethical issue. Additional concerns included equity (i.e., disparities in access to new technology creating biased datasets), risk of errors, and accountability (i.e., transparency or potential misappropriation of data).

Based on the findings from Taiwan, Dr. Wang provided the following recommendations to the Subcommittee: (1) Evaluate by reference to the counterfactual (i.e., what alternative technique could be used that is more desirable) to reduce burden and restrictions to the public and health care workers; (2) Consider the use of algorithms, particularly in respect to the appropriateness of implementing identified versus deidentified data; (3) Consider the use of electronic monitoring for support of confined individuals, to enforce restrictions on movement, and for contact tracing; (4) Obtain stakeholder input for the use of data with oversight to engender the trust of the public.

Discussion

Value of Contact Tracing Applications

Dr. Wang stated that the technology discussed during the presentations (i.e., smartphone tracking and applications) are necessary but are insufficient. He explained that Taiwan has a household registration, so the

government knows where everyone is supposed to be living. This registration allows for the chief of each district to assist individuals with their social service needs (e.g., groceries) while they are sick. However, he noted that tracking systems do allow the government to confirm that individuals in quarantine did not leave home, and therefore did not expose more members of the public to COVID-19—with breaking quarantine orders resulting in heavy fines for the individual so they are de-incentivized to leave home. Furthermore, Taiwan pays people $33 a day while they are in quarantine. All these factors mean there is a positive incentive to remain in quarantine.

Dr. Wang continued that, although insufficient, digital tracking may be necessary in the United States where there is no household registry. When in the United States, an individual cannot be tracked, raising concerns about potentially infecting individuals. He explained that exposure notification is a potential solution but the technology is insufficient on its own because it does not consider the human aspect of precautions (e.g., wearing protective gear, standing 6 feet apart).

Dr. Karras cited a model in Washington State that showed that only a 15% adoption of contact tracing apps could reduce deaths by 2-15%. He emphasized the need for public health responders to take every intervention that can be rolled into the existing toolkit for PHE response.

Mr. McDonald added that several deployments with greater than 15% uptake did not lead to a reduction of deaths as predicted by Dr. Karras' modeling. Many of the app owners have tempered expectations about the tools' helpfulness in reducing infections and deaths. He admitted that the tools should be studied further, but they are not meeting the needs of this pandemic. Instead, it would be worth investing in the infrastructure to ready the tools for future PHEs.

Dr. Gray added that the challenge of the proximity tracking apps is that they were not built to fit into the health care workflow. Until the toolkit identifies where the apps fit within the workflow to support public health response to PHEs, the apps will remain insufficient. She added that the workflow needs to contain more capabilities, such as identifying the social needs (e.g., grocery delivery) of individuals in quarantine. Until such additions are made to the workflow, they are useless to the large portion of the population—particularly non-white communities. She concluded that public health researchers should stop wasting time on the technologies and focus on investing in health care needs.

Dr. Gray noted examples of data trusts where groups have successfully engaged minority populations in the collection of data at the community level. She cited Harvard University, where students can see the data collected about them and how the data are used. She encouraged policies that allow individuals to control how aggregate data is repurposed.

Policy Changes

Dr. Karras stated that making the necessary changes to public health emergency response will require a multi-directional response that includes new laws and institutional infrastructure. He added that technology and law are meant to be reflective of productive relationships. Laws cannot create the relationships necessary to the success of public health methods. Mr. McDonald noted that existing technologies are assisting public health in noninvasive ways. The first action is to link development and deployment of technologies with a contextual relationship in communities.

Dr. Gray underscored that there is no such thing as deidentified data, which many policies rely on. She noted that many of the current policies in place or policies being discussed focus on the idea of creating deidentified data. She emphasized that focusing on the impossible goal of deidentified data is further eroding the public's trust. Instead she suggested rethinking and redefining working with data that are generating insights through aggregation that cannot be protected through deidentification. There are good examples within the government, such as the Census. In many ways, current practices are not respecting the rights of individuals. The public health field needs to find a way to engage with social exchanges rather than conducting large-scale surveillance and amassing large quantities of data.

Community Consent

Prof. Melissa Goldstein asked whether there are models of community consent, particularly in smaller communities. Dr. Gray described the Pandemic Response Network, part of Duke Health, which is working with community groups to position them as the beginning of contact tracing loops and patient support. In another example, 12 African American churches are acting as brokers in the community to manage the conversations around data collection and storage. This program shows that it is possible to create relationships in which a trusted data broker speaks for a community to ensure that data are used in their best interest and to educate individuals on the risks and benefits of the data collection. This approach will remove the ability to reuse data collected for other purposes, but it allows people to consent to each use of their data.

Mr. McDonald added that a lot of systems do not put a premium on validly collected data or necessary consent. To become a broker, individuals need to work in an ecosystem that puts individuals in the position to partake in publicly agreeable practice. Most places do not have those ecosystems available. Legal context needs to be established where these issues of trust and data collection are brokered.

Public Comments

Robert Gellman, privacy consultant in Washington D.C., informed the Subcommittee of a forthcoming report of relevance to the discussions. In partnership with Pam Dixon at the World Privacy Forum, Mr. Gellman is looking at the HHS responses to the COVID-19 pandemic. Mr. Gellman and Ms. Dixon have reviewed the authority of the waivers, the scope of the waivers, the process for issuing the waivers, and the underlying policies. Their report raises a series of questions that require attention once the bulk of the pandemic has been addressed. They suggest that the scope of HIPAA waivers belongs on that list of considerations, and the NCVHS may be the right organization to address that issue.

Jean Bikindou stated that he believes that the U.S. public is not confident that the government will protect them during the pandemic. He noted that the problem is the many apps, which can be used by many actors, to collect information. He stated that judicial law is important to regulate the use of these apps to protect the public and increase confidence about how the data will be used.

Jeffrey Abraham presented the following written comment for consideration via e-mail after the meeting: “I sincerely appreciate the opportunity to participate and listen in on this NCVHS Sub-Committee Hearing on Data Privacy, Confidentiality, and Security. I am looking forward to the report and forthcoming recommendations from this work. I look forward to participating in future NCHS/NCVHS activities as it directly impacts the COVID-19 work of myself and my fellow public health clinician-scientist colleagues.”

Subcommittee Discussion

Subcommittee Chair Frank Pasquale facilitated discussion with members. He noted the importance of creating and establishing resources as part of the overall framework for PHE response. Public health officials and other experts support the development of a well-funded, integrated, overarching response to PHEs at the local, state, and federal levels. This response requires a framework of social support that can be developed using models from successful jurisdictions to create a publicly trusted system. Prof. Pasquale noted that panelists were helpful in guiding the Subcommittee to move the field in the right direction.

The Subcommittee identified the following themes from the presentations:

- Data and data stewardship
- Coverage gaps
- Public trust
- Laws and policies

In addition to the summaries below, Prof. Pasquale requested that Subcommittee members send him three bullet points of the most important themes or recommendations that they believed were raised during the meeting.

Data and Data Stewardship

Key considerations regarding data stewardship raised during the meeting included:

- There is a need to consider data stewardship in the age of COVID-19 and how case examples can be applied to the gaps and needs.
- "Deidentification" is the backbone of much of the current public health data collection process. Terminology may need to change to accurately reflect the process of repackaging data for various purposes.
    - The field could also provide alternative models for promoting privacy.
- While a National Patient Identifier would be helpful, it is not a realistic goal as a focus for current efforts.
- There is need to consider how the field can increase the liquidity of data and the collection of key data—including better means of assessing and communicating the risks of different forms of data collection. Rapid response is critical in the context of emergencies.
- Often public health data are more secure than other public data because of the dedication of the individuals working with the data to the betterment of the public at large.
- Many smartphone apps require sign-up and download, providing a form of consent; however, there are concerns about secondary uses that are not anticipated by users.
- Prohibition of secondary use of data may help build public trust, if well enforced.
- NCVHS Subcommittee on Standards has a project under way about the convergence of clinical and administrative data—revisiting the fundamental premise of health care data between providers and payers—including public health data needs and the intersection of public health with the clinical and payer workflows.

Coverage Gaps

Key considerations regarding coverage gaps raised during the meeting included:

- Lack of payment coverage for testing
- Gaps in HIPAA privacy protection coverage
- The disparate impact on individuals partially caused by misidentification of individuals due to missing data in the analytical models.

Public Trust

Key considerations regarding public trust raised during the meeting included:

- Without public trust, no interventions or data collection efforts implemented in the public health field will be successful.
- When building a data trust, there is a need to consider the different responses to opt-in versus opt-out options and the balance between collecting the amount of data needed and maintaining public trust—for short-term and long-term data needs.
- Building public trust requires better ways to communicate the complex processes of data collection and storage so that the public can understand—with the person responsible sometimes likened to a data counselor.
    - Creation of this role will be challenging because the health care financial realm is encouraging hospitals to do more with less resources.
- Opt-in for all data use is complicated, and increased transparency is a complex lift for the field.
- Public distrust has been a longstanding, gradually worsening issue that cannot be addressed completely in the short term.
- Transparency is key to trust; however, speed is an important aspect of data collection, particularly related to vital statistics—quicker access to the data can help move along projects to address needs and build trust.
- Effective and clear emergency response with a sound scientific basis is the cornerstone on which public trust can be built.

Laws and Policies

Key considerations regarding laws and policies raised during the meeting included:

- Efforts should be made to create policies to address inconsistent, patchwork coverage across the nation by different state and local laws.
- National-level guidance may foster more consistency at the state and local levels.
- Laws should balance the need for privacy and protection of the individual with the need to collect data.
- The work recently completed by the NCVHS on Next Generation Vital Statistics could be used as a model to consider how working parts are being forced into an incomplete whole and how federal leadership can be supported to create a structure that can hold the disparate pieces together.

The Committee will use these ideas in combination with the ideas submitted to Prof. Frank Pasquale to serve as the basis for the Subcommittee's deliberations of recommendations at the next Subcommittee meeting.

Appendix A: Agenda

Monday, September 14, 2020

9:30 – 9:35 a.m. Welcome and Roll Call – Rebecca Hines, NCVHS Designated Federal Official

9:35 – 9:45 a.m. Opening Remarks – Frank Pasquale, Chair, PCS Subcommittee

9:45 – 10:00 a.m. Overview and Framing of Current Issues

10:00 – 11:30 a.m. Panel I – Data Collection and Use

- Ashkan Soltani, Independent researcher and technologist specializing in privacy, security, and technology policy. Former Senior Advisor to the U.S. Chief Technology Officer in the White House Office of Science and Technology Policy and as Chief Technologist for the Federal Trade Commission. [For the record: Contact-tracing apps are not a solution to the COVID-19 crisis]

- Commissioner Allison Arwady, Chicago Department of Public Health [Recommended viewing: https://www.nbcchicago.com/top-videos-home/arwady-explains-new-contact-tracing-efforts-in-chicago/2278204/]

- Robert Grossman, Co-Chief, Section of Computational Biomedicine and Biomedical Data Science, Dept. of Medicine; and Chief Research Informatics Officer (CRIO), Biological Sciences Division at the University of Chicago. [Recommended Reading: Rockefeller Foundation COVID-19 Testing Action Plan]

11:30 – 12:30 p.m. Break

12:30 – 2:00 p.m. Panel II – Technology and Ethics

- Professor Danielle Allen, Harvard University, Edmond J. Safra Center for Ethics [Recommended reading: Roadmap to Pandemic Resilience: Massive Scale Testing, Tracing, and Supported Isolation (TTSI) as the Path to Pandemic Resilience for a Free Society]

- John W. Loonsk, MD, Johns Hopkins University, Bloomberg School of Public Health and consulting chief medical informatics officer for the Association of Public Health Laboratories (APHL) [Recommended reading: Pandemic Reveals Public Health Data Infrastructure Shortcomings]

- Kate Goodin, Director, Surveillance Systems and Informatics Program, Communicable and Environmental Diseases and Emergency Preparedness, Tennessee Department of Health

- Stacey Mondschein Katz, Esq., Director of Healthcare Privacy and Human Protections Administrator, Maine Department of Health and Human Services

2:00 – 2:15 p.m. Break

2:15 – 3:45 p.m. Panel III — Bias and Discrimination

- Bryant Thomas Karras, M.D. Chief Informatics Officer, Office of the State Health Officer/Chief Science Officer, Washington State Department of Health
- Mary L. Gray, Senior Principal Researcher, Microsoft Research [Recommended reading: Mary Gray Urges COVID-19 Technology to Focus on Equity]
- Sean Martin McDonald, Senior Fellow, Centre for International Governance Innovation; Waterloo, Ontario, Canada [In the news: Contact-Tracing Apps Fail to Deliver on Tech Boosters' Promises]
- C. Jason Wang, MD, PhD, Director, Center for Policy, Outcomes and Prevention (CPOP), Stanford University [Recommended reading: Response to COVID-19 in Taiwan Big Data Analytics, New Technology, and Proactive Testing I JAMA]

3:45 – 4:00 p.m. Public Comment

4:00 – 4:15 p.m. Break

4:15 – 5:15 p.m. Subcommittee Discussion: Review themes, identify potential recommendations and additional information needs

5:15 p.m. Adjourn

Appendix B: Invited Speakers

Allison Arwady, Commissioner, Chicago Department of Public Health

Ashkan Soltani, Independent Researcher

Bryant Thomas Karras, Chief Informatics Officer, Washington State Department of Health

C. Jason Wang, Director, Center for Policy, Outcomes and Prevention, Stanford University

Danielle Allen, Professor, Harvard University

John W. Loonsk, Professor, Johns Hopkins University

Kate Goodin, Director, Surveillance Systems and Informatics Program, Tennessee Department of Health

Mary L. Gray, Senior Principal Researcher, Microsoft Research

Robert Grossman, Chief Research Informatics Officer, University of Chicago

Sean Martin McDonald, Senior Fellow, Centre for International Governance Innovation

Stacey Mondschein Katz, Esq., Director, Healthcare Privacy & Human Protections, Maine Department of HHS

Appendix C: Zoom Attendees

Adrienne Durham
Amelia Hood
Amy Chapper
Anna Marie
Bach Lin
Becky Lampkins
Brian Dehlinger
Candace Burton
Cassie Leonard
Charles Stellar
Charlie Chapin
Cheri Wilson
Chrystel Barron
Chynna Foucek
Cynthia Harry
Daniel Omondi
Danielle Lloyd
David Uberti
Debra Gilliam
Denise Chrysler
Dennis Garrett
Deven Desai
Fernando De Maio
Frank Pasquale
Gina Green-Harris
Griselle Torres
Heena Hameed
Jacqueline Green
James Sanderson
Janice Karin
Jean Bikindou
Jerry P Abraham
Joe Gibson
Joseph Rush
Julie Gregorio
Katelyn Ringrose
Kathryn Marchesini
Ken Johnson
Kim Williamson
Kyra Morgan
Laura Mayka
Laura Williamson
Laurie Darst
Lea Salvatore
Linda Sanches
Lisa Myers
Lisa Sloane
Liza Fuentes
Lobna Elsherif
Margaret Weiker
Marissa Gordon-Nguyen
Marissa Wong
Marny Burke
Matthew Downey
Matthew Garnett
Matthew Trunnell
Maya Ureño-Dembar
Meredith Massey
Meryl Bloomrosen
Micah Bass
Michele Dillon
Michele Suina
Michelle White
Mike Denison
Mildred Hunter
Myriam Hajaij
Natalie Gonzales
Nicholas Heesters
Nicole Toth
Olga Joos
Omenka Nwachukwu
Pamela Stephenson
Pat Yuzawa-rubin
Plamen Martinov
Pollyanna Sanderson
Robert Gellman
Sandeep Puri
Sandra Jamison
Sara Jordan
Sarah Colgan
Shouna Catanese
Urvi Sheth
Verne Rinker
Vivian Thomas
Wayne Wang
Weiwei Shen
Yoshi Tyler
Yvonne McHugh

Appendix D: List of Acronyms

API	Application Programming Interface
CECC	Central Epidemic Command Center
DP3T	Decentralised Privacy-Preserving Proximity Tracing
eCR	Electronic case reporting
EICR	Electronic Initial Case Report
ELR	Electronic laboratory reporting
HHS	U.S. Department of Health and Human Services
HIV	Human immunodeficiency virus
HIPAA	Health Insurance Portability and Accountability Act of 1996
IRB	Institutional Review Board
MeCDC	Maine Centers for Disease Control and Prevention
NCVHS	National Committee on Vital and Health Statistics
NEDSS	National Electronic Disease Surveillance System
PCS	Subcommittee on Privacy, Confidentiality and Security
PHE	Public Health Emergency
TEFCA	Trusted Exchange Framework and Common Agreement