NCVHS
National Committee on Vital and Health Statistics

December 15, 2022

The Honorable Xavier Becerra
Secretary
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: Recommendations regarding Privacy, Confidentiality, and Security Considerations for Data Collection and Use During a Public Health Emergency

Dear Mr. Secretary:

The National Committee on Vital and Health Statistics (NCVHS, Committee) is your advisory body on health data, statistics, privacy, and national health information policy. Over its more than 70-year history, the Committee has stimulated a range of improvements in national and international health data, data standards, and statistics. NCVHS is also charged with studying and identifying "privacy, security and access measures to protect individually identifiable health information in an environment of electronic networking and multiple uses of data."[1] Within the past two decades, NCVHS has advised the Secretaries on a range of matters regarding HIPAA's Privacy and Security Rules, offering advice on areas where protections can be improved.

The purpose of this letter is to provide recommendations to address privacy, confidentiality, and security of public health and healthcare data when collecting, using, and disclosing information during a public health emergency (PHE). On September 14, 2020, NCVHS convened a virtual hearing on Privacy, Confidentiality and Security Considerations for Data Collection and Use during a Public Health Emergency, consisting of three panels of experts.[2] The goal of the hearing was to seek input from public health practitioners, health care providers, and other experts regarding data privacy and security specifically in light of the COVID-19 PHE.[3] The Committee has reviewed input from written and oral testimony presented at the hearing, as well as from other published sources, to inform our recommendations for best practices, methods, and approaches to collecting, using, protecting, storing, and sharing of personally identifiable data during a pandemic or other long-term nationwide PHE.

---

[1] Charter, National Committee on Vital and Health Statistics (Jan. 21, 2022), *available at* https://ncvhs.hhs.gov/about/charter/ (visited May 17, 2022).

[2] NCVHS Virtual Hearing on Privacy, Confidentiality and Security Considerations for Data Collection and Use during a Public Health Emergency [2020 Hearing on PHE], September 20, 2020: https://ncvhs.hhs.gov/meetings/subcommittee-on-privacy-confidentiality-and-security-2/ (visited May 30, 2022).

[3] NCVHS, Final Agenda, 2020 Hearing on PHE, *available at* https://ncvhs.hhs.gov/wp-content/uploads/2020/09/Tentative-Agenda-NCVHS-PCS-Hearing-Data-Collection-and-Use-during-PHE-as-of-09-11-2020_508.pdf (visited May 30, 2022).

The meeting's objectives focused on:

- Understanding policies and practices involving data collection, use, and disclosure with respect to privacy and security during the COVID-19 PHE;
- Understanding 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
- Identifying best practices and areas where additional technical assistance or guidance from HHS may be useful.

The Committee approached this hearing at a time when technologies, methodologies, and other approaches for collecting data about the COVID-19 pandemic were evolving in the United States and around the world. As NCVHS was planning this hearing during the summer of 2020, new technologies for contact tracing and exposure notification were emerging, both inside and outside the United States. Multiple entities, governmental and private, were developing other methodologies to gather patient data individually and at the population level to assess COVID's impact on health needs. Public health agencies, researchers, clinicians, and others were eager to improve public health surveillance techniques for monitoring individuals to better understand morbidity and mortality associated with this novel virus. The press as well as data privacy experts raised concerns about particular practices and asserted the need for greater guardrails on the collection and use of personally identifiable data.[4]

In preparation for the September 2020 hearing, the Committee asked panelists to consider several questions. We were interested in their perspectives on methodologies for data collection and use during the COVID-19 PHE. We were also interested in understanding what privacy and security safeguards could be considered to enhance public trust and better safeguard individually identifiable information. Based on lessons learned from the hearing, as well as a consideration of reports developed on this topic by a variety of other organizations, NCVHS makes the following recommendations to HHS:

Recommendation 1. Develop a national governance strategy specific to PHEs in collaboration with federal, tribal, state, territorial, and local partners that increases trustworthiness in data collectors, data stewards, and those who share the data collected in and after the PHE.

Recommendation 2. As part of this data governance strategy, develop data stewardship responsibilities, based on fair information principles, for all entities collecting, using, and sharing data during a PHE.

Recommendation 3: Support the development of accelerated interoperable information sharing for PHEs that prioritizes privacy and security.

---

[4] *See* Trump Administration Strips C.D.C. of Control of Coronavirus Data, *The New York Times* (July 14, 2020), https://www.nytimes.com/2020/07/14/us/politics/trump-cdc-coronavirus.html; Disappearance of covid-19 data from CDC website spurs outcry, *Washington Post*, July 16, 2020: https://www.washingtonpost.com/health/2020/07/16/coronavirus-hospitalization-data-outcry/; Irregularities In COVID Reporting Contract Award Process Raise New Questions, *National Public Radio*, July 29, 2021: https://www.npr.org/2020/07/29/896645314/irregularities-in-covid-reporting-contract-award-process-raises-new-questions (visited May 30, 2020).

Recommendation 4. Review the current process for issuance of PHE waivers, Notices of Enforcement Discretion, and sub-regulatory guidance.

Recommendation 5. Address inequities in the collection and timely reporting of datapoints on disaggregated race, ethnicity, geography, and age in use now and in the future at the federal, tribal, state, territorial, and local levels.

Attached you will find detailed justifications for each of our recommendations in the Appendix.

As the healthcare ecosystem continues to address the pandemic, it is important that we do not lose sight of lessons to be learned from this experience so that we may be better prepared for future PHEs. It is critical that HHS give attention to improving data flows within and between healthcare and public health and among agencies at all levels of government while maintaining a privacy appropriate environment. The Committee notes that data governance and management challenges often outpace issuance of regulations or are outside the scope of current jurisdiction. As always, NCVHS underscores the importance of principle-based information practices: all stewards of personal health information must embed strong privacy and security standards into their products and services. It is in this spirit of learning that the Committee offers these recommendations, and NCVHS looks forward to working with the Department.

Sincerely,

[redacted]

Jacki Monson, J.D., Chair
National Committee on Vital and Health Statistics

Enclosure

Cc: Benjamin Sommers, ASPE
Melanie Fontes Rainer, OCR
Chiquita Brooks-LaSure, CMS
Micky Tripathi, ONC
Roselyn Tso, IHS
Rochelle Walensky, CDC

APPENDIX

Justification for Recommendations regarding Privacy, Confidentiality, and Security Considerations for Data Collection and Use During a Public Health Emergency

Based on lessons learned from the NCVHS hearing, as well as consideration of reports developed on this topic by a variety of other organizations, NCVHS makes the following recommendations to HHS:

Recommendation 1. Develop a national governance strategy specific to PHEs in collaboration with federal, tribal, state, territorial and local partners that increases trustworthiness in data collectors, data stewards, and those who share the data collected in and after the PHE.

"Data governance is the framework or structure for ensuring that an agencies' data assets are transparent, accessible, and of sufficient quality to support its mission, improve the efficiency and effectiveness of agency operations, and provide useful information to the public."[5] The COVID-19 pandemic has underscored the urgency for HHS to develop a governance strategy specific to PHEs with measures that ensure the privacy and security of data, promote trust, and demonstrate the trustworthiness of data collectors and data stewards and those who, in addressing the PHE, share the data.

Trustworthiness includes the ability of those who give their data to determine that the potential benefit to society is greater than the potential harms they as individuals may encounter. The Public Health Code of Ethics requires that our public health efforts are guided by the idea that "the effectiveness of public health policies, practices, and actions depends upon public trust gained through decisions based on the highest ethical, scientific, and professional standards."[6] In the case of a PHE, trustworthiness requires consistency with the Belmont Report[7] and other principles of ethical research, recognizing that public health surveillance itself is not research. Such a principle means that public health officials strive to avoid exposing individuals to unnecessary risks but, in a PHE, limited exposure to privacy risks is sometimes considered acceptable if that exposure can be predicted to bring sizable benefits based on evidence-based practice. Trustworthiness includes transparent processes so that individuals are making informed, voluntary decisions after an opportunity to weigh the potential benefits and the burden of risk attached to providing their data in the service of addressing the PHE.[8] NCVHS recommends that HHS develop a national data governance strategy that is overarching, integrated across data platforms and agencies, well-resourced, and socially interoperable at all levels of

---

[5] U.S. Gov't Accountability Office, *DATA GOVERNANCE: Agencies Made Progress in Establishing Governance, but Need to Address Key Milestones* (Dec. 2020), at 4-5. https://www.gao.gov/products/gao-21-152 (visited May 17, 2022).

[6] Public Health Code of Ethics. American Public Health Association. https://www.apha.org/-/media/files/pdf/membergroups/ethics/code_of_ethics.ashx (2019)(visited May 30, 2022).

[7] Nat'l Comm'n for the Protection of Human Subjects of Biomedical and Behavioral Research, THE BELMONT REPORT: ETHICAL PRINCIPLES AND GUIDELINES FOR THE PROTECTION OF HUMAN SUBJECTS OF RESEARCH (Dep't of Health, Ed. & Welfare, April 18, 1979) *available at* https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html (visited May 30, 2022).

[8] See, e.g., Alicia L. Best et al., Institutional Distrust among African Americans and Building Trustworthiness in the COVID-19 Response: Implications for Ethical Public Health Practice, 32 *J. Health Care for the Poor and Underserved* 90-98 (Johns Hopkins U. Press, Feb. 2021), *available at* https://muse.jhu.edu/article/783096/pdf (including, among other recommendations, that "public health and medical institutions should prioritize structural competency and transparency," to develop trustworthiness) (visited May 30, 2022).

government — federal, tribal, state, territorial, and local. The strategy should recognize both the benefits and possible risks of data collection and use and should account for the use of new technologies to collect, anonymize, and share clinical, hospitalization, surveillance, vital records, and other health data in a timely manner. NCVHS recommends that HHS consider the importance of the management of public health data initially collected in a PHE throughout that data's life cycle, including privacy and security protections that build and maintain public trust and enable the permissions to use and share such data.

We have learned from other infectious disease outbreaks and natural disasters, such as the human immunodeficiency virus (HIV), Ebola, and Zika epidemics, or Hurricanes Katrina, Irma, Maria, and Ian, that governmental entities, healthcare organizations, and others need easy and rapid access to public health data to support public health surveillance, research, policymaking, public communication, and decisions about allocation of resources. Data-driven public health policy decisions are only possible if the data is efficiently collected from the public, accurate and of high-quality, shared in a timely manner, and protected appropriately.

NCVHS also recognizes the need for improved information system capabilities in public health agencies. The Committee recommends that HHS develop a governance strategy at the national level to facilitate both ease of access and creation of privacy and security guardrails to ensure that data collected during PHEs are accessible, when appropriate, and in a form that can help with timely decision-making. One of the panelists at the September 2020 hearing noted that, unlike countries with national healthcare systems, the U.S. system's decentralized nature has forced state and local public health departments to gather information from different health data and government silos to gain a patchwork picture of their residents' health.[9] This process can result in losing precious time for controlling the spread of an epidemic. This panelist also emphasized that her organization strives to "bake in" privacy and security, and that both must be embedded into local public health organizations' policies and practices even as they scramble to keep up with the rapid pace of technology.[10] That attention is particularly necessary in a PHE as relaxation of enforcement designed to ensure protection and privacy of data are sometimes employed for purposes of expediency and to extend access to data to others when needed to respond during a PHE.

Additionally, to help support clarity of roles in data sharing and reduce duplication of data collection efforts, NCVHS recommends that HHS provide guidance on the role of HIPAA business associates[11]

---

[9] 2020 Hearing on PHE, Statement of Dr. Allison Arwady, at 21.

[10] *Id.*

[11] Business Associate is defined in the HIPAA Regulations as follows:

Business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

> **(ii)** Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

during future PHEs. In early 2020, when COVID-19 data collection efforts were less organized and more hurried, the Office for Civil Rights (OCR) issued a Notification of Enforcement Discretion (NED) to announce that it would not penalize health care providers or their business associates for violations of certain HIPAA provisions if a business associate, in good faith, disclosed protected health information (PHI) for public health and health oversight activities even if outside of the scope of their formalized business associate agreement (BAA).[12] This NED was issued quickly to allow business associates to disclose data to public health agencies and other organizations working to contain the pandemic. At the time, at least one electronic health record organization wrote to the hospital covered entities (CEs) with which it had business associate agreements notifying them that it would send their data to the CDC and state and local public health organizations to which the hospitals were obligated to provide reports.[13] The message was not a request to health care providers for permission to disclose the information, but a statement that the information in their systems would be disclosed without an opportunity to opt out. While most of the CEs did not object, some larger hospital systems already had efforts underway to release the same information, so the actions of the business associate had the potential to duplicate in-process disclosures, increase processing time for the public health recipients, and compromise data quality.

This NED potentially set a precedent that could create conflicts between CEs and their business associates in the future. Covered entities rely on business associate agreements to manage their data and IT environment by establishing requirements, controlling permissions, and mitigating legal liability, even during PHEs. NCVHS recommends that HHS provide guidance that clearly outlines the roles of business associates during future PHEs, including requiring permission from a covered entity to release information on its behalf if that release of information will help rapidly address data needs. The guidance should also consider the varying nature of local and global PHEs and methods to avoid duplication of effort.

Key to the success of any governance strategy is to develop “trustworthiness” on behalf of those whose data is being shared. While current data governance strategies focus on increasing the level of trust among those whose data are sought, to be productive, these efforts must include the development of principles and methods that can demonstrate to the public that data stewards, collectors, and sharers are trustworthy.[14] This can be accomplished by embedding data security, protection and privacy methods, being transparent about data use, and managing the lifecycle of the data with protection and transparency in mind.

---

45 CFR § 160.103.

[12] HHS, Ofc. for Civil Rts., Press Release: OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency,” (Apr. 2, 2020) *available at* https://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html; Ofc. of the Sec’y of HHS, “Enforcement Discretion Under HIPAA To Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID–19, 85 Fed. Reg. 19392-93 (Apr. 7, 2020) *available at* https://www.govinfo.gov/content/pkg/FR-2020-04-07/pdf/2020-07268.pdf (visited May 30, 2022).

[13] See, e.g. Adam Cancryn, “Kushner’s team seeks national coronavirus surveillance system,” *Politico* (Apr. 8, 2020), *available at* http://www.politico.com/news/2020/04/07/kushner-coronavirus-surveillance-174165 (visited May 17, 2022).

[14] Griffith, et al., (https://link.springer.com/article/10.1007/s11606-020-05868-1; http://www.ihi.org/communities/blogs/its-not-you-its-us-earning-trust-to-build-community-connections)

Recommendation 2. As part of this data governance strategy, develop data stewardship responsibilities, based on fair information principles, for all entities collecting, using, and sharing data during a PHE.

NCVHS encourages HHS to define and employ data stewardship based on fair information principles[15] for all entities collecting, using, or linking to data systems during a PHE. For example, the Department could draw on principles of fairness derived from health information ethics, such as those developed in 2008 by the Office of the National Coordinator for Health Information Technology (ONC) in its work on the electronic exchange of health information.[16] ONC identified eight principles: 1) Individual Access, 2) Correction; 3) Openness and Transparency; 4) Individual Choice; 5) Collection, Use, and Disclosure Limitation; 6) Data Quality and Integrity; 7) Safeguards; and 8) Accountability. Data stewardship responsibilities should always, even in the face of a PHE, adhere to fair information principles. While allowances may need to be made by HHS for certain entities, when a PHE occurs, it is critical that the Department return to the fundamental importance of fair information principles. The importance of these responsibilities should be widely disseminated by the Department to all entities to raise awareness about the risks and potential consequences of misuse and reuse of data, including re-identification, to individuals, vulnerable groups, and establishments.

Based on panelist input at the hearing, NCVHS has also discussed the need for revisiting the HIPAA de-identification standard, which is heavily relied upon in use of administrative data. NCVHS suggests that

---

[15] The original Code of Fair Information Practice was developed by one of the most influential federal advisory committees ever convened, the Department of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems. Its Code included five elements:

1. There must be no personal data record-keeping systems whose very existence is secret;
2. There must be a way for an individual to find out what information about him is in a record and how it is used;
3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent;
4. There must be a way for an individual to correct or amend a record of identifiable information about him; and
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (Dep't of HEW, July 1973). This Code forms the basis of the federal Privacy Act of 1974, 5 U.S.C. 552a, and virtually all data protections laws around the world since its issuance.

[16] Office of the Nat'l Coord. for Health Info. Tech, HHS, "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information" (Dec. 15, 2008) *available at* https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf (visited May 17, 2022). Following this effort, OCR in 2010 issued Frequent Asked Questions (FAQ) endorsing the principles and explaining how they related to the HIPAA Privacy and Security Rules. Following the passage of the Patient Protection and Affordable Care Act (ACA), Pub. L. 111–148, 124 Stat. 119 (Mar. 23, 2010), CMS incorporated these same principles into its ACA final rule on "General Standards on the Establishment of an Exchange," 45 CFR § 155.260, setting minimum requirements for safeguarding the privacy of exchange related PII. *See also* Centers for Medicare and Medicaid Services (CMS), HHS, Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement Version 1.0, at 16 (Aug. 1, 2012), https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Harmonized-Security-and-Privacy-Framework-ERA-Supp-v-1-0-08012012-a.pdf (visited Sep. 13, 2022).

the advent of new technologies provides the opportunity to explore new models for de-identification that should be assessed by HHS. The Committee has done a significant amount of past work on de-identification and provided comprehensive recommendations on this issue to the HHS Secretary in 2017.[17] It is worth noting that, to date, HHS has not followed up on these recommendations. Furthermore, one of the panelists at the September 2020 hearing noted that, "overreliance on deidentification alone and the trafficking in large scale data without the public's buy-in, arguably without their understanding, is risking further erosion of the public's trust, and we can't afford this in the second and third wave of this pandemic or future pandemics."[18]

Data stewards should also focus on uses of data that go beyond the original purpose for which they were collected. NCVHS has previously published guidance describing the difference between original and repurposed data,[19] and endorses the importance of purpose specification.[20] For example, individual genomic information collected initially upon COVID-19 testing to identify variants and severity levels for effective treatment might also be used in an unethical and discriminatory manner if not properly controlled. Genomic data can yield a wealth of information when analyzed to make predictions about the individual data subject, those related to the individual, and others who have affiliations with the individual based on ethnicity, racial or cultural background. These potential uses should be considered prior to the data collection, if possible, or at the least, prior to repurposing after the initial reason for collection has been satisfied.[21]

To promote greater understanding, trustworthiness, and transparency, NCVHS recommends that HHS make every effort to communicate to the public expectations of good data stewardship, data protection practices, and methods for reporting any perceived abuse of data collected or used during a PHE. Good data stewardship will include methods, even in the face of regulatory enforcement relaxation, to protect data from misuse or unapproved re-use. Stewardship practices must include procedures to assess at regular intervals whether methods employed by data stewards continue to be appropriate. These might include, for example, the use of algorithms in decision-making, the methods of estimation of resource allocation, evaluation of the extent to which linkages and re-use are endangering the privacy and security of personal information, or revisiting equity markers of prevention, mitigation, or treatment during a PHE. A steward's actions should be guided by the growing public expectation that individuals will be informed about how their data are being used and disclosed, with what parties it is shared, and how it is protected.

Recommendation 3: Support the development of accelerated interoperable information sharing for PHEs that prioritizes privacy and security.

Private and secure standards-based sharing of patient data across public health and healthcare systems and organizations (what is often referred to as "interoperability") is widely recognized as part of the

---

[17] NCVHS' Recommendations on De-identification of Protected Health Information under HIPAA, February 23, 2017: https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf

[18] 2020 Hearing on PHE, Statement of Dr. Mary Gray, at 86.

[19] NCVHS, "Toolkit for Communities Using Health Data: How to collect, use, protect and share data responsibly," at 11," *available at* https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/Toolkit-for-Communities.pdf (visited May 17, 2020).

[20] *Id*. at 29-32.

[21] Gyngell, C., et al., "Ethically utilising COVID-19 host-genomic data," 6 *npj Genom. Med.* 31 (May 10, 2021), *available at* https://www.nature.com/articles/s41525-021-00194-9 (visited Sept 13, 2022).

solution to improving outcomes for individuals and populations. Time is of the essence. Data should reach its users as close to real time as feasible given the systems involved and the specific use case for that data transfer.

Interoperability includes health data exchange architecture and standards which enable data to be accessed and shared appropriately and securely across the spectrum of care within applicable settings and with relevant stakeholders, including the individual, and getting the right data to the right person at the right time. The COVID-19 pandemic has made it clear that healthcare providers and public health agencies alike must be more effective in managing data and ensuring that it is available as close to real time as feasible to better understand morbidity and mortality during emerging outbreaks. A public health official at the September 2020 hearing mentioned the limited interoperability among states and the insufficient state funding for modernization to accommodate new standards.[22] The need for an interoperable healthcare system that effectively integrates public health information is evident. Accelerating the development of an interoperable system for PHEs is an investment that can build our capacity for preparedness.

The Committee notes that a major challenge to interoperability is the persistence of data silos in multiple components of the health system, which hinders the transfer of data across public health entities at all levels of government. For example, during the hearing the Chicago Department of Public Health shared its difficult experience prior to the pandemic of matching children who have lead poisoning with participants in the housing choice voucher program due to restrictions on data sharing across platforms.[23] During the COVID-19 pandemic, data silos in the healthcare, public health, vital records, and public assistance systems have posed a significant challenge to targeting public health interventions efficiently and effectively.[24] Several panelists at the hearing suggested bridging these silos or even breaking them down to enable an effective public health response.[25] The lack of shared patient data during a PHE due to data silos is a significant risk to effective disease control and limits our country's ability to manage an outbreak collectively so that it does not become a nationwide, or indeed global, pandemic. The following practices may support more efficient and effective information sharing during a PHE while respecting the privacy of the patients whose personally identifiable data are the basis of any successful strategy:

- Strengthening the Immunization Information Systems (IIS), also known as Vaccine Registries, including increased linkage between IIS and electronic health records[26]
- Developing a standardized data use agreement. Discussions in the hearing featured the Trusted Exchange Framework and Common Agreement (TEFCA) as well as Maine CDC's Data Sharing and Protection Agreement, both of which illustrate the benefits of having a standardized agreement for data sharing parameters.[27]

---

[22] 2020 Hearing on PHE, testimony of Kate Goodin, at 74.

[23] *Id.*, testimony of Allison Arwady, at 34.

[24] *Id.*, at 21. *See also*, Kate Jercich, "What we've learned so far from the COVID-19 pandemic," *Healthcare IT News* (Aug. 10, 2021), *available at* https://www.healthcareitnews.com/news/what-weve-learned-so-far-covid-19-pandemic (visited June 5, 2022).

[25] 2020 Hearing on PHE, testimony of Allison Arwady, at 21; testimony of Robert Grossman at 26-30, 35; testimony of Stacey Mondschein Katz at 66.

[26] See CDC, About Immunization Information Systems (June 7, 2019).https://www.cdc.gov/vaccines/programs/iis/about.html (visited Jan. 12, 2022).

[27] 2020 Hearing on PHE, Statement of Dr. Robert Grossman, at 28-29; Statement of Dr. John Loonsk, at 55; Statement of Stacey Mondschein Katz, at 69.

- Creating data commons platforms that combine data and computing infrastructures. A data commons can balance patient data protections with open research that benefits patients.[28] The National Institutes of Health (NIH) has created multiple data commons platforms that illustrate their benefits to the larger research community in the everyday and PHE settings.[29] In addition, the Rockefeller Foundation's report advocating for a national COVID-19 testing and tracing action plan includes a recommendation to create a data commons platform that balances data privacy and security with data utility.[30]
- Sharing data within communities in a privacy-appropriate, secure, and ethical environment
- Providing effective privacy and security guidelines for the life cycle of collection/creation, maintenance/security, use, disclosure/sharing, and eventual disposition.
- Collecting and sharing of complete demographic data, including disaggregated information on age, geography, race, ethnicity, and, when available, sexual orientation and gender identity (SOGI) and social determinants of health (SDOH).

Recommendation 4. Review the current process for issuance of PHE waivers, Notices of Enforcement Discretion, and sub-regulatory guidance.

In this section we make the following recommendations regarding the effect of a PHE declaration on statutory waivers under section 1135 of the Social Security Act and Notices of Enforcement Discretion (NEDs), administrative actions with respect to HIPAA:

- Ensure that the Department carefully limits waivers or NEDs that remove important protections for patient privacy during declarations of emergency to the period necessary for governance of each emergency.
- Ensure that the Department conducts careful monitoring and evaluation of industry activities during the pendency of all waivers or NEDs to ensure patients are not being unduly deprived of important rights.

When the President declares an emergency, under Section 319 of the Public Health Service (PHS) Act, the Secretary of HHS may declare a PHE if the Secretary determines, after consulting with such public

---

[28] See 2020 Hearing on PHE, Statement of Dr. Robert Grossman, at 27.

[29] *See, e.g.*, Patricia A. Deverka et al., "Creating a data resource: what will it take to build a medical information commons?" 9 Genome Medicine art. 84 (2017), *available at* https://genomemedicine.biomedcentral.com/articles/10.1186/s13073-017-0476-3 (describing eight core principles proposed by a diverse group of expert stakeholders to guide the formation of a successful, sustainable medical information commons); NIH, Data Commons Pilot: Program Snapshot (May 13, 2019) *available at* https://commonfund.nih.gov/commons (The NIH Data Commons Pilot Phase explored new ways to store, access, and share biomedical data and associated tools in the cloud so they were FAIR. Not to be confused with Fair Information Principles, in the research context, FAIR is an acronym standing for Findability, Accessibility, Interoperability, and Reusability—it does not include principles usually associated with privacy or confidentiality.); (visited May 30, 2022). *See also*, Robert Cook Deegan et al., "Introduction: Sharing Data in a Medical Information Commons, 47 J. of Law, Med. & Ethics 7-11 (2019), *available at* https://journals.sagepub.com/doi/full/10.1177/1073110519840479 (visited June 5, 2022).

[30] The Rockefeller Foundation, "National COVID-19 Testing Action Plan: Pragmatic steps to reopen our workplaces and communities," (April 21, 2020), a*vailable at* https://www.rockefellerfoundation.org/wp-content/uploads/2020/04/TheRockefellerFoundation_WhitePaper_Covid19_4_21_2020.pdf (visited Sep. 13, 2022).

health officials as may be necessary that:

1) a disease or disorder presents a PHE, or
2) a PHE, including significant outbreaks of infectious diseases or bioterrorist attacks, otherwise exists.[31]

A PHE declaration allows the Secretary to take certain actions in response to the PHE. These actions may include waivers under section 1135 of the Social Security Act (SSA) of requirements otherwise imposed on some regulated entities.[32] The waivers are available to hospitals that have implemented a disaster protocol[33] from being subject to sanctions and penalties for non-compliance with requirements during a public health emergency when it is most difficult to comply.

Under this authority, HHS waives sanctions and penalties arising from noncompliance with the privacy regulations relating to:

- the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care[34]
- the requirement to honor a request to opt out of the facility directory[35]
- the requirement to distribute a notice of privacy practices [36]
- the patient's right to request privacy restrictions [37]
- the patient's right to request confidential communications[38]

HHS's practice is to automatically activate a waiver in the emergency region for the statutory maximum period — 72 hours, and that time begins to run once a hospital has implemented its disaster protocol.[39]

In addition to the statutory 1135 waivers, during the COVID 19 PHE, OCR also issued several NEDs to grant additional flexibilities to all HIPAA covered entities and their business associates. NEDs eliminate the risk of sanctions and penalties, for example, against a covered insurer that is unable to comply with certain provisions of the Privacy Rule due to the emergency. These actions have been more long-lasting than a typical Section 1135 waiver. OCR has stated that it believes that the NEDs are a statement of agency policy, not subject to the notice and comment requirements of the Administrative Procedure Act (APA).[40] OCR also asserts that even if such guidance were subject to the public participation provisions

---

[31] 42 U.S.C. § 247d(a).

[32] Social Security Act § 1135 *available at* https://www.ssa.gov/OP_Home/ssact/title11/1135.htm, codified at 42 U.S.C. 1320b–5 *available at* https://www.govinfo.gov/content/pkg/USCODE-2020-title42/pdf/USCODE-2020-title42-chap7-subchapXI-partA-sec1320b-5.pdf (visited Oct. 24, 2022).

[33] Under 42 U.S.C. § 247d(d) the Secretary may also grant an extension of a deadline to submit required data and may waive any sanctions for failure to comply.

[34] 45 CFR 164.510(b)

[35] 45 CFR 164.510(a)

[36] 45 CFR 164.520

[37] 45 CFR 164.522(a)

[38] 45 CFR 164.522(b)

[39] *See Administration for Strategic Preparedness and Response,* Public Health Emergency Declaration Q&As (reviewed Sept. 5, 2019), *available at* https://www.phe.gov/Preparedness/legal/Pages/phe-qa.aspx (last visited Nov. 4, 2022).

[40] Each of the NEDs includes this footnote:

> "Due to the public health emergency posed by COVID-19, the HHS Office for Civil Rights (OCR) is exercising its enforcement discretion under the conditions outlined herein. We

of the APA,[41] prior notice and comment for this type of guidance is impracticable, and there is good cause to issue NEDs without prior public comment and without a delayed effective date.[42]

There have been several NEDS issued by OCR during the COVID-19 PHE. The first one makes it easier to provide telehealth services during the emergency. This Notification applies to all HIPAA-covered health care providers, with no limitation on the patients they serve with telehealth, including those patients that receive Medicare or Medicaid benefits. Covered health care providers will not be subject to penalties for violations of the HIPAA Privacy, Security, and Breach Notification Rules that occur in the good faith provision of telehealth during the COVID-19 PHE. However, OCR encouraged providers to notify patients that these third-party applications potentially introduce privacy risks and suggested that providers enable all available encryption and privacy modes when using such applications.

Another NED issued during the COVID-19 PHE suspends penalties for violations of the HIPAA Rules in connection with the good faith operation of community-based COVID-19 testing sites during the PHE.[43] The third Notification issued during the COVID-19 PHE suspends penalties for violations of certain provisions of the HIPAA Privacy Rule for the good faith use or disclosure of PHI by business associates for public health and health oversight activities during the PHE.[44]

All NEDs remain in effect until the end of the COVID-19 PHE. OCR has pledged to issue a notice to the public when it is no longer exercising this enforcement discretion based upon the latest facts and circumstances.[45]

When the Secretary declares a PHE, the Public Health Service Act limits its duration to 90 days, after which it automatically expires.[46] The law contemplates an event of limited geographic and temporal scope, such as one after a fire or other natural disaster, not an event of indefinite time, such as what we are experiencing with the COVID-19 pandemic. In the case of COVID-19, HHS has renewed the PHE declaration every 90 days since the first declaration in January 2020.[47] While the statutory 1135

> believe that this guidance is a statement of agency policy not subject to the notice and comment requirements of the Administrative Procedure Act (APA). 5 U.S.C. 553(b)(A). OCR additionally finds that, even if this guidance were subject to the public participation provisions of the APA, prior notice and comment for this guidance is impracticable, and there is good cause to issue this guidance without prior public comment and without a delayed effective date. 5 U.S.C. 553(b)(B) & (d)(3)."

[41] *See* Administrative Procedure Act, 5 U.S.C. 553(b)(3)(B) & (d)(3).

[42] A full list of OCR's Bulletins in response to various HIPAA PHE waivers may be found here: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html, and the list of OCR announcements related to COVID-19 and HIPAA may be found here: https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html (both visited Nov. 4, 2022).

[43] OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency | HHS.gov (pagefreezer.com)

[44] OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency | HHS.gov (pagefreezer.com)

[45] OCR, "FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency," *available at* https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf (visited June 6, 2022).

[46] Public Health Service Act, § 319, 42 U.S.C. § 247d.

[47] Secretary of HHS, Renewal of Determination That a Public Health Emergency Exists, HHS (Oct. 15, 2021), *available at* https://www.phe.gov/emergency/news/healthactions/phe/Pages/COVDI-15Oct21.aspx (visited June 6, 2022).

waivers were valid only for 72 hours, the administratively established NEDs have continued throughout the pandemic, even though their necessity may have faded over time. In addition, some commenters have criticized their legal foundation.[48]

In the early months of the pandemic, the Secretary typically waited until days before the expiration of the PHE declaration before issuing a renewal, a practice that raised questions and concerns about the possibility of stakeholders needing to rapidly unwind dozens of administrative functions with little warning. On January 22, 2021, the Acting HHS Secretary sent a letter to governors[49] stating that "the PHE will likely remain in place for the entirety of 2021, and when a decision is made to terminate the declaration or let it expire, HHS will provide states with 60 days' notice prior to termination." The letter acknowledges the importance of "predictability and stability" for states' emergency planning efforts and notifies governors to "expect the continued use of other emergency authorities" that are not expressly linked to the PHE declaration.

The Committee commends HHS for its foresight in issuing this letter but urges the agency to develop a long-term process for ensuring that waivers or NEDs that remove important protections for patient privacy during declarations of emergency are carefully limited to the period necessary for governance of each emergency and that careful monitoring and evaluation of industry activities during these periods is performed.

Recommendation 5. Address inequities in the collection and timely reporting of datapoints on disaggregated race, ethnicity, geography, and age in use now and in the future at the federal, tribal, state, territorial and local levels.

COVID-19 has had an unprecedented and disproportionate impact on racial and ethnic minorities and low-income individuals, from higher rates of infection, illness, and death to greater social and financial hardships.[50] Access to timely and accurate data is fundamental to identifying disparities in PHEs and advancing health equity to address the disparities expeditiously. Data helps the healthcare industry and responsible public health entities identify where disparities exist, tailor efforts and resources, measure efficacy, and establish accountability for achieving progress to reduce and mitigate preventable morbidity and mortality. Without granular, individual-level data, inequities will remain unaddressed, and preventable morbidity and mortality in these populations will continue disproportionately.

The Centers for Disease Control and Prevention (CDC) reports the race and ethnicity of people vaccinated at the national level, but race and ethnicity data is still — at this late date in the pandemic — missing for 22.4% of fully vaccinated people over the age of five and of 25.7% of those who have

---

[48] *See, e.g.,* Robert Gellman and Pam Dixon, "COVID-19 and HIPAA: HHS's Troubled Approach to Waiving Privacy and Security Rules for the Pandemic," World Privacy Forum (Sept. 16, 2020), *available at* https://www.worldprivacyforum.org/2020/09/covid-19-and-hipaa/ (visited June 5, 2022).

[49] Office of the Asst Sec'y for Preparedness and Response, U.S. Dept. of Health and Human Services, Public Health Emergency Declarations: Letter to Governors on COVID-19 Response, https://www.phe.gov/emergency/news/healthactions/phe/Pages/default.aspx

[50] *See* Simmons A, et al., "Health Disparities by Race and Ethnicity During the COVID-19 Pandemic: Current Evidence and Policy Approaches," Ofc. of the Asst. Sec'y for Planning & Eval., HHS (Mar. 16, 2021) *available at* https://aspe.hhs.gov/sites/default/files/migrated_legacy_files/199516/covid-equity-issue-brief.pdf; Mays, Vickie M., et al., "Data Equity in American Indian/Alaska Native Populations: Respecting Sovereign Nations' Right to Meaningful and Usable COVID-19 Data," 112 Am. J. Public Health 1416 (October 2022) (both visited Nov. 4, 2022).

received at least one dose of a COVID-19 vaccine.[51] For several months at the beginning of the pandemic, it was reported that race/ethnicity data was missing in as many as 50% of cases.[52] Moreover, CDC is not publicly reporting vaccinations by race/ethnicity designated by state, limiting our understanding of how disparities may still vary across the country. While the number of cases of COVID-19 have decreased from the earlier times in the pandemic public health surveillance is still charged with monitoring surges and increases in cases. Delays in obtaining race and ethnicity are delays in both seeing patterns of inequities in the continuation of COVID-19 cases as well as providing testing, treatment, and care. In the absence of CDC reports, the Kaiser Family Foundation has conducted an analysis of state-reported data on COVID-19 vaccinations by race/ethnicity.[53] However, this effort is impeded by inconsistencies in how states report their data and the speed at which they provide it. Unlike data reported by the CDC, which is standardized, states vary in the racial/ethnic classifications they use, their units of measure, and their frequency of reporting, among other factors. As one of the panelists on an NCVHS panel earlier this year on COVID and race/ethnicity pointed out, as a goal, all states need to employ the Census 2020 population denominators in their calculation of any COVID-related rates for the ability to compare across states.[54] The panelist noted, however, that there are several state dashboards that are still using old population denominators from 2018 and 2019.

NCVHS recommends that HHS accelerate work to assist the development of standardized state-based reporting, including guidance on categories for the classification of race, ethnicity, age (especially ages of children); how these data are reported; and timeliness in the sharing of these data in PHEs. Increased standardization of disaggregated racial and ethnic data will aid the industry and public health agencies in analyzing and interpreting all manner of health status and healthcare data.

In addition, the Office of Management and Budget (OMB) sets minimum standards for reporting race and ethnicity data that were last revised in 1997 and may not fully reflect the diversity of today's population.[55] For example, data collection should include smaller groups than are currently accounted for, such as American Indian and Alaska Native and Native Hawaiian and Other Pacific Islander people, as well as subpopulations of the broader racial and ethnic categories of people who have migrated in

---

[51] CDC, "Demographic Characteristics of People Receiving COVID-19 Vaccinations in the United States," *available at* https://covid.cdc.gov/covid-data-tracker/#vaccination-demographic (a set of maps, charts, and data updated daily by 8:00 PM in the eastern US time zone (visited Sept. 13, 2022).

[52] Krieger, N., et al., US Racial and Ethnic Data for COVID Still Missing in Action, 396 *The Lancet* 10261, at E81 (Nov. 7, 2020).

[53] Latest Data on COVID-19 Vaccinations by Race/Ethnicity, Kaiser Family Foundation, November 3, 2021: https://www.kff.org/coronavirus-covid-19/issue-brief/latest-data-on-covid-19-vaccinations-by-race-ethnicity/; *See also* The COVID Tracking Project published by *The Atlantic available at* https://covidtracking.com/race and its COVID Racial Tracker, which includes State Reporting Assessments, *available at* https://covidtracking.com/about-data/state-reporting-assessments (visited September 13, 2022).

[54] NCVHS, **Follow-up Panel on Covid-19: Capacity, Gaps & Quality in Collection of Race/Ethnicity Data (Jan. 25, 2022) ["Jan. 2022 panel"] Statement of** Elizabeth Pathak, at 5. The agenda, transcript, and recording of this meeting may be found at https://ncvhs.hhs.gov/meetings/full-committee-meeting-9/ (visited June 7, 2022).

[55] Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity, Office of Management and Budget (Oct. 30, 1997), *available at* https://www.govinfo.gov/content/pkg/FR-1997-10-30/pdf/97-28653.pdf (visited Nov. 7, 2022).

more recent years to the United States.[56] We do understand, however, that additional safeguards will need to be taken to protect the privacy of the data originating within these smaller subpopulations. Updated standards for reporting of race and ethnicity data should facilitate consistent and timely reporting at all levels of government.

NCVHS is also concerned about standards that support the reporting of cases by age. A panelist at the January 2022, panel stated that, for example, Texas reports total case counts to the CDC, but does not include age.[57] The differences in state dashboards versus that which is reported to the CDC is another area of concern. Many state dashboards will use 0-17 as a bucketed range for reporting age while the CDC restricted use file uses 0-19, so that the two datasets are difficult to compare and produce accurate estimates. Another panelist at the January 2022 panel noted that the Florida dashboard appears to be missing race and ethnicity data for only 12.4 percent of child cases, but is missing that data in approximately 35 percent of all cases in its reporting of child cases to the CDC.[58] This results in inaccurate statistical reporting on the CDC COVID Tracker website for case incidence by age and race/ethnicity.

As reported by one of the panelists at the 2020 Hearing on PHE, there are states in which almost all state case-demographic data are missing.[59] In some states, cases were missing age or race/ethnicity, and in other cases this data was missing on the CDC COVID Tracker or in the case line files. The implication of this is that the CDC COVID Tracker can report an erroneous tally of COVID-19 cases particularly by race, ethnicity, or age for children and adolescents.[60] At the same time, the panelist noted that in several cases states report more cases stratified by demographics on their own dashboards than are either reported to, or included by, CDC on its own COVID Tracker dashboard. Reconciling local data versus data reported to the CDC is critical because the CDC uses the data from the states to advise the nation. If race, ethnicity, age, or geographic indictors are missing, then CDC will be unable to consider issues specific to racial and ethnic subpopulations, thus increasing inequity in the experience of these subpopulations due to a PHE in comparison to more complete data in other populations. The goal must be to have uniform, highly consistent, thorough reporting of both the underlying cases, the denominators, and race and ethnicity.

To reach these goals, CDC may need to support reengineering and modernizing data collection and reporting systems and structures to allow for more timely disaggregated data reporting.[61] States and

---

[56] Grantmakers in Health and the Nat'l Comm. for Quality Assurance, Improving Data on Race and Ethnicity: A Roadmap to Measure and Advance Health Equity (Dec. 2021), *available at* https://www.gih.org/wp-content/uploads/2021/12/GIH-Commonwealth-Fund-federal-data-report-part-2.pdf (visited June 7, 2021). *See, for example*, HHS Implementation Guidance on Data Collection Standards for Race, Ethnicity, Sex, Primary Language, and Disability Status (Oct. 30, 2011), *available at* https://aspe.hhs.gov/reports/hhs-implementation-guidance-data-collection-standards-race-ethnicity-sex-primary-language-disability-0 (visited Nov. 7, 2022). The HHS guidelines use more granular categories that may be aggregated into the minimum categories required by OMB.

[57] Jan. 2022, panel, Statement of Elizabeth Pathak, at 5.

[58] January 2022 panel, Elizabeth Pathak, at 6.

[59] *Id*.; Mays, Vickie M., et al., The Accumulation of Disadvantage: Black Children, Adolescents, and COVID-19 Data Inequity. 112 Am. J. Public Health 1407 (Oct 2022).

[60] *Id.*

[61] See CDC, "Data Modernization — COVID Guidance: Project C2" (July 21, 2021) https://www.cdc.gov/ncezid/dpei/pdf/data-modernization-508.pdf (visited Nov 4, 2022). *See also* J.T. Lane, et al., "COVID-19 Highlights Critical Need for Public Health Data Modernization to Remain a Priority," 26 J. Public Health

localities may also need to reexamine their privacy laws and adopt technology that can collect and link needed demographic data for use in PHEs. There are states that have gone beyond HIPAA and created privacy protections for health data maintained by non-HIPAA covered entities as part of their consumer protection legislation.[62] For example, as described by the Association for State and Territorial Health Officials, [63] Oregon passed a law adopting "requirements on developing and implementing COVID-19 contact tracing applications and other technologies, limiting the storage of personal health data to 65 days."[64]

Finally, NCVHS notes that about half of the states and some other countries have adopted strategies for selecting and deploying technologies for exposure notification,[65] and some have also adopted applications for vaccine scheduling. However, if implemented more broadly in the United States, even if those strategies could have overcome the multiple challenges they faced,[66] they would have allowed many people to be left behind, including those who cannot use the technology because of lack of access to broadband or due to geographic or financial reasons. While NCVHS began its investigation about privacy and the PHE focused on the use of technology in COVID-19 exposure notification and surveillance, we found these strategies not to be in widespread use in the United States. There are, nonetheless, equity issues in the use of technology in the United States in the few small instances observed but also for potentially more widespread deployment in future PHEs. In a PHE, the use of technology may provide benefits for rapid notification, public health surveillance, and even access to healthcare (such as via telehealth) that could improve the protection and prevention of morbidity and mortality in an infectious disease outbreak. However, HHS and other public health entities should pay attention to how access to and utilization of technologies such as broadband, smartphones, voluntary databases registrations such as V-Safe,[67] public health notifications, and other applications may differ by race, ethnicity, geography, age, and other characteristics found to

---

Manag. & Pract. 6 (Nov/Dec 2020), *available at* https://journals.lww.com/jphmp/Fulltext/2020/11000/COVID_19_Highlights_Critical_Need_for_Public.21.aspx (visited Sept. 13, 2022); Brownson, Ross C., et al., Reimagining Public Health in the Aftermath of a Pandemic," 110 Am. J. Public Health 165 (Nov. 2020) *available at* https://ajph.aphapublications.org/doi/full/10.2105/AJPH.2020.305861 (visited Nov. 4, 2022).

[62] Cite state consumer privacy law with "beyond HIPAA" protections

[63] ASTHO, *Public Health for the 21st Century: Data Modernization and Privacy Protections* (Legislative Overview Series: 2022 Public Health Spotlight), *available at* https://www.astho.org/globalassets/pdf/legislative-prospectus_data-modernization.pdf.

[64] *See, e.g.,* section 3, chapter 305, Oregon Laws 2021, codified at Or. Rev. Stat. § 646.607 (June 16, 2021)(prohibiting covered organization from collecting, using or disclosing personal health data about resident individual who has not given affirmative express consent for collection, use or disclosure unless in context of employment relationship or to comply with legal obligation, or unless personal health data was lawfully available to public from federal, state or local government records, was collected before emergency period for reasons other than tracking, monitoring or tracing resident individual's exposure to or infection by SARS-CoV-2 or COVID-19 or has been deidentified in accordance with federal law) *available at* *https://www.oregonlegislature.gov/bills_laws/ors/ors646.html* (visited Sept 13, 2022). Note that the Oregon amendments become operative on the date that is 450 days after the date of the termination or expiration of the emergency declared by the Governor related to the COVID-19 pandemic. The text of House Bill 3284 that contained this provision may be found here: https://gov.oregonlive.com/bill/2021/HB3284/

[65] *See* GAO, *Exposure Notification: Benefits and Challenges of Smartphone Applications to Augment Contact Tracing (***Sept. 9, 2021)**, *available at* https://www.gao.gov/products/gao-21-104622 (visited Nov. 21, 2022).

[66] *Id.*

[67] See CDC, V-Safe After Vaccination Health Checker, https://www.cdc.gov/coronavirus/2019-ncov/vaccines/safety/vsafe.html (last updated July 18, 2022, visited Nov. 7, 2022).

cluster in socially vulnerable populations. In the interest of preparedness for the next PHE, we recommend continued examination of how technologies are performing, who has the capacity to use them, and the appropriateness of such uses with respect to privacy, security, and confidentiality for these vulnerable populations.