ConnectedHealthInitiative

February 28, 2022

Lawrence A. Tabak, D.D.S., Ph.D.
Acting Director
National Institute of Health
Department of Health and Human Services
6705 Rockledge Drive, Suite 750
Bethesda, Maryland 20892

RE: Comments of the Connected Health Initiative on *Request for Information on Proposed Updates and Long-Term Considerations for the NIH Genomic Data Sharing Policy* (NOT-OD-22-029)

Dear Dr. Tabak:

The Connected Health Initiative (CHI) appreciates the opportunity to provide input on the National Institutes of Health's (NIH) Request for Information on Proposed Updates and Long-Term Considerations for the NIH Genomic Data Sharing (GDS) Policy, intended to maximize scientific advances and public benefit by sharing genomic data and associated phenotypic data in a manner consistent with participants' informed consent.[1] CHI supports NIH's effort to ensure policies around genomic data sharing keep pace with evolving scientific opportunities and stakeholder expectations.

CHI represents a broad consensus of stakeholders across the healthcare and technology sectors whose mission is to support the responsible and secure use of connected health innovations throughout the continuum of care to improve patients' and consumers' experience and health outcomes. We advocate before the Department of Health and Human Services (HHS) on realizing the benefits of an information and communications technology-enabled American healthcare system. CHI is committed to advancing an interoperable healthcare system that enables the bidirectional flow of necessary health data, including genomic data, between provider and patient, as well as between other important stakeholders who have a role in improving care coordination and decision-making.

The efficacy of precision medicine, population health, clinical decision support—and artificial/augmented intelligence (AI)-driven tools in particular—is dependent in large part on the availability of massive data sets. The free flow of information and interoperability are therefore important and potentially life-saving for patients. While the

[1] NOT-OD-22-029 (Nov. 30, 2021).

types of data items analyzed by AI and other technologies are not new, this analysis provides greater potential utility of those data items to other individuals, entities, and machines. Thus, there are many new uses for, and ways to analyze, the collected data. This raises privacy issues and questions surrounding consent to use data in a particular way (e.g., research, commercial product/service development). It also offers the potential for more powerful and granular access controls for patients. Accordingly, any policy framework should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process.

NIH's proposed policy comes at an important time. Advances in computing and related reductions in the cost of genomic sequencing has led to an explosion of available data. NIH's GDS Policy must be updated to allow for greater information sharing if researchers and care providers are going to effectively use genomic data to advance patient care. Based on this, we provide the following viewpoints and recommendations on NIH's proposed updates to the GDS Policy:

- CHI is supportive of NIH's consideration of aligning the GDS Policy with the HIPAA Privacy Rule (45 CFR 164.514(b)(1)). Increased alignment with the HIPAA Privacy Rule, by allowing expert determination in assessing de-identification, will increase flexibility for those working with genomic data (who currently have only one method for de-identification) while maintaining participants' privacy.

- NIH's GDS policy should be scalable and assure that an individual's health information is properly protected, while also allowing the flow of health information that is necessary to provide and promote high-quality healthcare and to protect the public's health and well-being. We agree that genomic data requires additional policy safeguards given that one individual's DNA includes potentially identifying information about even distant relatives of that individual, necessitating a separate approach and enhanced protection from discrimination based on pre-existing conditions or genomic information may be needed for patients.

  For example, fully leveraging technical measures including end-to-end encryption is a critical element to protecting data broadly, enabling key segments of the economy—from banking to national security to healthcare—by protecting access to, and the integrity of, data. Encryption's role should not be understated – without encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised. The U.S. government already plays an important role in promoting the use of encryption, e.g., the National Institute of Standards and Technology's (NIST's) Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry,

government, and academia.[2] NIST also provides the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography-based standards.[3]

- CHI generally supports NIH's efforts to respect the autonomy and privacy of research participants and protection of confidential data. Connected datasets are a critical tool for researchers looking to advance research using the latest analysis techniques and for the development of digital health applications, particularly those enabled by the implementation of artificial intelligence. These modern tools improve patient care and outcomes across a range of medical disciplines. To realize the full benefits of advances in genomic sequencing, combining genomic data acquired with informed consent with data elements considered potentially identifiable should be allowed. This includes allowing for links between GDS-compliant datasets and those that do not meet all GDS Policy expectations.

- CHI encourages NIH to continue its efforts to harmonize its data sharing policies with others in the healthcare space. Such harmonization reduces administrative burdens and reduces confusion for both research participants and researchers. Harmonization of data sharing rules will help to encourage more information sharing between parties while ensuring that genomic data privacy is maintained. We urge NIH to align its policies with the efforts of other key health sector agencies to reduce the burden on researchers linking datasets, and to ensure consistent rules for participant privacy.

  Further, we urge NIH to align with risk management guidelines and standards developed by the NIST with respect to electronic health records,[4] and general information security standards and guidelines for federal agencies,[5] including the NIST Cybersecurity Framework[6] and the National Strategy for Trusted Identities in Cyberspace (NSTIC).[7]

- CHI is broadly supportive of NIH's effort to harmonize the GDS Policy with the DMS Plans while recognizing that some policies will need to remain in the GDS

---

[2] *See* http://csrc.nist.gov/.

[3] *See* http://csrc.nist.gov/groups/STM/cmvp/.

[4] NIST's roles in this context have been articulated in both Federal Health IT strategic plans (2008–2012 and 2011–2015) and in the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009.

[5] Title III of the E-Government Act of 2002 (P.L. 107-347).

[6] http://www.nist.gov/cyberframework/index.cfm.

[7] http://www.nist.gov/nstic/.

Policy that are not found in more general data management plans due to the sensitive nature of genomic data. Such harmonization reduces administrative burdens and reduces confusion for both research participants and researchers. Harmonization of data sharing rules will help to encourage more information sharing between parties while ensuring that genomic data privacy is maintained. A logical, objective approach is necessary to reduce confusion, and NIH should further align its genomic data sharing policy with the Office of the National Coordinator for Health IT's (ONC's) information blocking to the extent possible. While this rule is currently approaching finalization, it will represent the baseline for information sharing moving forward, and NIH should align its data management and sharing policies with these rules to the maximum extent possible to provide continuity across the healthcare ecosystem. For example, CHI recommends use of the Fast Healthcare Interoperable Resources (FHIR) standard (Release 4) as well as HL7 U.S. Core FHIR Implementation Guides (or in the alternative that NIH permit the use of such widely-accepted standardized approaches to information sharing). Data sharing timelines should be harmonized between the GDS Policy and DMS Plans to reduce confusion, particularly in the case where a dataset contains more than genomic data.

- CHI generally supports preserving and sharing data through established repositories using a common data access agreement consistent with the GDS Policy, but also encourages enabling APIs to facilitate streamlined data flows. NIH's GDS Policy completely omits discussion of APIs and how NIH contemplates APIs playing a role in its sharing of data. We believe this is an oversight that NIH needs to address before its policy is finalized. We strongly encourage NIH to facilitate the use of two-way APIs for management and sharing of data.

CHI appreciates the opportunity to submit its comments to NIH. We look forward to assisting NIH in modernizing and improving its genomic data sharing policy.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Leanna Wade
Policy Associate

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005