



PUBLIC RESPONSIBILITY IN
MEDICINE AND RESEARCH

June 20, 2022

Chair

F. Claire Hankenson, DVM,
MS, DACLAM

Vice Chair

Robert Nobles, DrPH, MPH

Secretary

Megan Kasimatis Singleton,
JD, MBE, CIP

Treasurer

Jori Leszczynski, DVM,
DACLAM

Members

Allyson J. Bennett, PhD

Brenda Curtis, PhD, MsPH

Mary L. Gray, PhD

David Augustin Hodge, Sr.,
DMin, PhD

Martha Jones, MA, CIP

David Litwack, PhD

Holly Fernandez Lynch,
JD, MBE

Vickie M. Mays, PhD, MSPH

Gianna McMillan, MA, DBE

Helen O'Meara,
MS, CPIA, LSSGB

Suzanne Rivera, PhD, MSW

Stephen Rosenfeld, MD

Ex Officio

Elisa A. Hurley, PhD

Lawrence Tabak, DDS, PhD
Acting Director
Office of the Director
National Institutes of Health
9000 Rockville Pike
Rockville, MD 20892

Submitted electronically at <https://osp.od.nih.gov/rfc-draft-supplemental-information-to-the-nih-policy-for-dms/>

RE: NOT-OD-22-131: Request for Public Comments on DRAFT Supplemental Information to the NIH Policy for Data Management and Sharing: Protecting Privacy When Sharing Human Research Participant Data

Dear Dr. Tabak,

Public Responsibility in Medicine and Research (PRIM&R) appreciates the opportunity to comment on the DRAFT *Supplemental Information to the NIH Policy for Data Management and Sharing: Protecting Privacy When Sharing Human Research Participant Data*, published on May 12, 2022.

PRIM&R is a nonprofit organization dedicated to advancing the highest ethical standards in the conduct of research. Since 1974, PRIM&R has served as a professional home and trusted thought leader for the research protections community. Through educational programming, professional development opportunities, and public policy initiatives, PRIM&R seeks to ensure that all stakeholders in the research enterprise appreciate the central importance of ethics to the advancement of science.

PRIM&R appreciates the NIH effort to provide the research community with a set of principles, best practices, and points to consider for creating a robust framework for protecting the privacy of research participants when sharing data under the NIH Policy for Data Management and Sharing. The research community is eager for NIH's guidance and leadership in this area. ***However, we believe that the current draft is not fully developed and does not achieve the stated goal. The information provided is vague and perfunctory, at best, which diminishes its usefulness to the research community in establishing best practices for protecting the privacy of research participants.***

Below are PRIM&R comments on specific sections of the draft:

I. DRAFT Operational Principles for Protecting Participant Privacy When Sharing Scientific Data

The introduction to this section includes the phrase “Respect for and protection of participant privacy is the foundation of the biomedical and behavioral research enterprise.” PRIM&R notes that “respect for and protection of participant privacy” is *not* in fact the, or even a, foundational principle of the research enterprise, and referring to it as such undermines the authority of this document. The NIH has an opportunity here to educate the research community about how and why practices that respect and protect participant privacy, while not foundational, derive from the widely recognized, understood, and accepted research ethics principles of the Belmont Report, namely, Respect for Persons, Beneficence, and Justice.

Furthermore, we note that none of the seven “principles” are truly overarching principles, but rather comprise simple directives using ambiguous terminology and authoritative statements. For example:

(4) Institutional review of the conditions for data sharing, including that proposed limitations on the future use of data are appropriate and that risks have been considered. Limitations should be conveyed with the data when they are transferred, such as when sharing through repositories to secondary users.

As written, this can be interpreted as requiring institutional review boards (IRBs) to review data sharing plans even if the research does not meet the regulatory definition of human subjects research (HSR). NIH needs to clarify whether IRBs are expected to review data sharing plans even when the research does not meet the federal regulatory definition of HSR.

(5) Collection of data from non-traditional research settings, such as mobile health devices, social media, consumer reports, and public health surveillance also warrant strict privacy considerations.

The category of “social media” today is broad and spans the private-public continuum. Thus, inclusion of data from social media without any qualifiers is inappropriate. In addition, the phrase “warrant strict privacy considerations” is vague and unhelpful without further elucidation of what NIH considers those considerations to be.

(6) There may be justifiable exceptions to sharing scientific data, regardless of the sufficiency of access controls and de-identification techniques. In these rare instances, researchers should outline these justifications in their Data Management and Sharing Plans.

In the absence of a definition or examples, it is not clear how the research community is to determine what instances constitute “justifiable exceptions.” The reference cited for additional information on justifiable reasons for limiting sharing of data under the DMS Policy does not in fact provide any, except in the instance that the research is cofunded by a private sector entity that has applied restrictions on data sharing as a condition of funding. Thus, NIH should provide examples of a variety of cases that meet this standard.

(7) Responsible data sharing practices require a commitment from the entirety of the biomedical and behavioral research enterprise. Researchers and institutions should remain vigilant regarding potential misuse and work in concert with NIH to prevent unauthorized use of scientific data from NIH-supported platforms and repositories. In addition, NIH is committed to enforcing the terms of its data use agreements

It is unclear how researchers and institutions would “remain vigilant” about potential misuses of data that are deposited in repositories. Once data are deposited, with a description of

limitations on future use, if any, the original researchers and institutions are not responsible for the day-to-day governance of datasets in the repository. Thus, the onus for ensuring that data are not misused in the future should be on the entity that manages the repository and not on the researchers and their institutions.

II. DRAFT Best Practices for Protecting Participant Privacy When Sharing Scientific Data

PRIM&R applauds NIH for explicitly acknowledging that in the age of big data, de-identification of data has become more difficult, if not impossible, and for recommending the use of new computational approaches to secure privacy. Given the changing research landscape wherein many entities not covered under the HIPAA privacy rule (including technology companies) collect, store, and share personal health information¹, we recommend that HIPAA not be identified as a best practice for protecting participant privacy. And with reference to the last bullet, the research community would greatly benefit from examples of what constitutes “other relevant protections.”

***Establish Scientific Data Sharing and Use Agreements.** NIH recommends the use of scientific data sharing and/or use agreements, preferably standardized, when sharing data from participants with and from repositories.*

It is unclear who is responsible for developing “standardized” data sharing and/or use agreements, the criteria to be used for developing a standardized agreement, and how a standardized form would be adapted to different types of data (fully open, limited access, etc.)

***Understand Legal Protections Against Disclosure and Misuse.** Per the NIH Certificates of Confidentiality Policy, data subject to the Policy are deemed issued a Certificate of Confidentiality, including some data that have been de-identified (e.g., human genomic data). Certificates of Confidentiality protect the privacy of research participants by prohibiting disclosure of protected information for non-research purposes to anyone not connected with the research except in specific situations. Protections afforded by Certificates apply to all copies of a dataset in perpetuity.*

The language in this section is confusing. Given that NIH automatically issues Certificates of Confidentiality (CoC) for supported research that collects or uses identifiable sensitive information, perhaps the recommendation should instead be that researchers and institutions ensure that the repository where the data are deposited is aware that the data are protected by a CoC.

III. DRAFT Points to Consider for Designating Scientific Data for Controlled Access

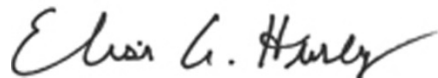
PRIM&R believes that this section is the most useful in providing practical guidance on measures that researchers can take to share sensitive data while also protecting the privacy of participants. That said, the section could be improved by providing the research community, in point #3, examples of measures, other than access controls, that can mitigate the risk of re-identification.

¹ <https://www.theregreview.org/2021/08/20/tovino-hipaa-strengths-and-limitations/>

In closing, as we have expressed before, PRIM&R recognizes the enormous potential benefit of data sharing, and supports the wide sharing of data among researchers as one means by which research participants can be sure that their contributions to science and society are maximized.² PRIM&R urges the NIH to consider re-drafting the guidance so that NIH-funded researchers and institutions have a clear understanding of how to meet the NIH standards for protecting the privacy of research participants while following the agency's DMS Policy. We believe that the sections on best practices and points to consider should be further developed based on our comments and comments from the larger research community. The guidance should not just allude to all relevant regulations and policies, but identify and incorporate requirements of those policies and regulations in the practical measures that researchers can employ to ensure privacy. Furthermore, the utility of the guidance would be greatly enhanced by the use of more unambiguous language and concrete examples that clearly illustrate potential options applicable to different types of data.

Thank you again for the opportunity to comment on the *DRAFT Supplemental Information to the NIH Policy for Data Management and Sharing: Protecting Privacy When Sharing Human Research Participant Data*. We hope our comments are useful in your next stage of policymaking in this area. PRIM&R stands ready to provide any further assistance or input on this important issue. Please feel free to contact me at 617.303.1872 or ehurley@primr.org.

Sincerely,



Elisa A. Hurley, PhD
Executive Director

cc: PRIM&R Public Policy Committee, PRIM&R Board of Directors

² See, for instance, PRIM&R's comments in response to the 2019 Draft NIH Policy for Data Management and Sharing and Supplemental Draft Guidance: <https://primr.org/getmedia/e0b4bf13-8baf-4aef-b3c3-5533ca5a7db3/01-10-20-PRIMR-Comments-January-10-final.pdf>.