



June 24, 2022

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

Office of the Director
National Institutes of Health
9000 Rockville Pike
Bethesda, MD 20892

RE: Comments in Response to NIH Guide Notice NOT-OD-22-131

To Whom It May Concern:

The Council on Governmental Relations (COGR) is an association of nearly 200 public and private U.S. research universities and affiliated academic medical centers and research institutes. COGR concerns itself with the impact of federal regulations, policies, and practices on the performance of research conducted at its member institutions. One area of expertise among COGR members is human subjects research protections, including protections for the use and sharing of data collected from research participants.

COGR appreciates the opportunity afforded by NIH to comment on the *Draft Supplemental Information for Data Management and Sharing: Protecting Privacy When Sharing Human Research Participant Data* notice (hereafter "[NOT-OD-22-131](#)" or "Notice"). COGR members appreciate the importance of data sharing to scientific advancement, as well as the need to provide appropriate protections for the data that is being shared, particularly with respect to guarding the privacy and confidentiality of human research participants. COGR appreciates NIH's development of the draft operational principles, best practices, and points to consider outlined in NOT-OD-22-131, and below we provide our comments on these items for NIH's consideration. In our comments, we include, for ready reference, the text of the draft principle, practice, or point for consideration, but with footnotes omitted.

Overall Purpose of NOT-OD-22-131

NOT-OD-22-131 is framed as "supplemental information" to the [NIH Policy for Data Management and Sharing](#) ("DMS Policy"). NOT-OD-22-131 states that it is not a "guide for compliance with regulatory requirements," but rather a "set of principles, best practices, and points to consider for creating a robust framework" (emphasis added) for protecting the privacy of research participant data shared under the DMS Policy. COGR applauds the Notice's flexible approach of framing its provisions as considerations, not requirements. We also support NIH's statement in footnote two that the principles are "not intended to address data security standards." We would, of course, expect that any new data security standards would be issued through standard

rulemaking processes, particularly security standards governing de-identified data obtained from fundamental research, two areas for which long-standing regulations exist.

Comments on DRAFT Operational Principles for Protecting Participant Privacy When Sharing Scientific Data

DRAFT Principle 2: *Researchers and institutions should proactively assess appropriate protections for sharing scientific data from participants, including determining whether sharing should be restricted through controlled access, regardless of whether the data meet technical and/or legal definitions of “de-identified” and can legally be shared without additional protections (e.g., the research does not meet the definition of “human subjects research” under the Common Rule).*

COGR appreciates the need for institutions and researchers to consider “appropriate protections” when sharing human research participants’ data. In discussing the potential need for “controlled access,” however, the definition of that term (and the term “access controls”) in footnote four references only verification of identity and “appropriateness” of proposed research as examples of possible controls. No additional detail is provided about how such verification should be accomplished or what proposed research or researchers might be considered “inappropriate.” We request that NIH provide additional detail about criteria institutions might use to assess “appropriateness,” as NIH uses that term in the Notice. Further, if NIH is considering limitations on requesters (e.g., limitation by type or location of researcher) or the type of research for which data may be shared, we ask that such limitations be clearly stated. Although we concur that proactive assessment of the need for additional protections is beneficial, Principle 2 should explicitly acknowledge that there are instances in which additional controls are neither necessary nor advisable, and that technical and legal definitions, although not necessarily conclusive, remain relevant in this analysis.

DRAFT Principle 3: *Investigators and institutions should develop robust consent processes that prioritize clarity regarding future sharing and use of scientific data, including limitations on future use, and general aspects regarding how data will be managed (see *Informed Consent for Secondary Research with Data and Biospecimens: Points to Consider and Sample Language for Future Use and/or Sharing*). Importantly, when a study offers the possibility of a direct benefit for research participants, the DMS Policy does not require sharing of data in order to participate.*

COGR supports robust informed consent processes that describe both potential risks and benefits of study participation, including those stemming from the use and disclosure of data. Indeed, studies have shown that research participants broadly support data sharing from research in which they participate,¹ and informed consent processes should take such views into consideration. Further, the way in which data is shared may present not only risks and benefits to subjects, but also affect the study as a whole. For example, participant consent to data sharing may be necessary in certain types of research (e.g., sponsored clinical trials of drug and device products) to avoid the risk of incorrect/incomplete data analysis. Principle 3 does not address this larger context.

¹ See, e.g., Mello, M., et. al., [Clinical Trial Participants Views of the Risks and Benefits of Data Sharing](#), 372 N. Engl. J. of Med., 2202 (June 7, 2018).

Rather, it has a narrow, and somewhat puzzling focus, on the DMS Policy statement that data sharing is not required to participate in a study offering direct benefit to participants. COGR suggests that NIH modify Principle 3 by deleting the last sentence and substituting the following text: “Importantly, in developing plans for future data use and describing such use in the informed consent process, researchers should consider: (a) risks and benefits to participants; (b) impact of data sharing restrictions on the study and utility of the data; and (b) all data sharing requirements that may apply (e.g., requirements of the DMS Policy, [clinicaltrials.gov](https://www.clinicaltrials.gov), other regulatory agencies, and study sponsors or funders), including those that do/do not mandate data sharing as a requirement of participation.”

DRAFT Principle 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.*

COGR fully supports NIH’s consideration of exceptions to broad data sharing, and we urge NIH to ensure that its institutes and centers take a consistent approach in evaluating and permitting such exceptions. We also request that NIH provide guidance as to how such exception will be considered when Data Management and Sharing Plans are evaluated.

Comments on DRAFT Best Practices for Protecting Participant Privacy When Sharing Scientific Data:

DRAFT Best Practice 1: *Ensure Appropriate De-identification.* *NIH recommends scientific data to be de-identified to the greatest extent possible in a manner that maintains sufficient scientific utility. Researchers and institutions should consider the following strategies and their appropriateness given their particular research and scientific data:*

- *Relying on the standards for identifiability outlined in the Common Rule (participant identity cannot “readily be ascertained”) and in the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (i.e., Expert Determination or Safe Harbor), regardless of whether these rules apply to the sharing, disclosure, or subsequent use of data.*
- *As methods for re-identifying individuals continue to become increasingly sophisticated and available for use, employing advanced statistical or computational methods to de-identify data and maintain privacy whenever feasible and appropriate.*
- *In some cases, scientific utility may be lost if shared data are de-identified. It may consequently be justifiable in certain cases to share scientific data under the DMS Policy that meet a legal or regulatory standard for identifiability. In those cases, data sharing may be subject to particular rules, and researchers should also consider whether other relevant protections should be employed.*

The 2018 revisions to the Common Rule (or “Rule”) outline the role federal agencies play with respect to the “identifiability” of information. Specifically, agencies implementing the Common Rule “shall” consult with experts to “reexamine the meaning of ‘identifiable private information’”²

² 45 C.F.R. § 46.102.

within one year of the Rule's effective date, and at least every four years thereafter. Institutions have anticipated that OHRP would work with agencies to carry out the Rule's mandate to convene experts to "assess whether there are analytic technologies or techniques that should be considered by investigators to generate 'identifiable private information'" and include these technologies/techniques on a list to be published in the Federal Register for public comment. The Notice, however, makes no mention of these specific regulatory responsibilities on the part of federal agencies implementing the Common Rule. We request that NIH revise this best practice to address federal agencies' role in the reexamination of "identifiability" and how the results of such reexamination will shape any requirement to use advanced deidentification methods. Specifically, we recommend that NIH convene an expert panel task force to examine common methods of deidentification and common new technologies that may produce identifiable data and then make the determinations required by 45 C.F.R. § 46.102(e)(7). This process will provide uniformity and expert informed guidance to institutions.

DRAFT Best Practice 2: *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. These agreements should be considered even if scientific data are de-identified and should be negotiated among researchers, institutions, and repositories. Key elements that promote the privacy of research participants in such agreements include:*

- ***Oversight.*** *Agreements should clearly include certification from an institutional official that, at a minimum, scientific data have been appropriately de-identified (and to which standard), that an institutional oversight body has reviewed and considered the risks of data sharing, and that sharing is consistent with informed consent (as applicable).*
- ***Responsibilities.*** *Agreements should delineate responsibilities of all parties having access to the data and clearly inform parties on data use limitations as well as responsibilities regarding privacy and confidentiality, including those required by Certificates of Confidentiality, as applicable.*
- ***Restrictions.*** *Agreements should explicitly outline sharing limitations and explicitly prohibit attempts to re-identify and/or recontact participants or their family members unless there is explicit agreement to do so. Such restrictions should travel with the data.*

COGR appreciates NIH's flexibility in recommending, rather than mandating, the use of data use agreements and/or the listed key elements. However, we are concerned about this Practice's introduction of the concept of an institutional certification encompassing de-identification (including the appropriateness of the standard used), review by an institutional oversight body, and consistency of the proposed data sharing with informed consent provisions. COGR agrees that data use agreements should clearly describe: (a) how data has been de-identified; (b) the institutional review performed; and (c) the specifics of any informed consent governing the data, but we disagree with the recommendation that an institutional certification is always necessary or appropriate. Rather, certifications and similar statements (e.g., warranties and representations) and their attendant liabilities should be the product of negotiation among the parties to a data use agreement, and will, of necessity, vary depending on the data, uses, and parties involved (e.g., public entities, private institutions, etc.). A blanket recommendation for institutional certification in all cases does not account for this wide variety of circumstances, and therefore, is inappropriate.

In this respect we note that such a certification concept is absent from both the HIPAA implementation standards for de-identification³ and data use agreements.⁴

DRAFT Best Practice 3: *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.*

First, we note that the title for Best Practice 3 is not accurate because the practice does not provide a comprehensive list of all legal protections that may apply. Thus, we recommend that NIH delete the title “Understand Legal Protections Against Disclosure and Misuse” and replace it with “Understand Certificate of Confidentiality Protections Against Disclosure and Misuse.”

Second, Certificates of Confidentiality have limited utility as data protection tools because their use and protections are restricted to cases of compelled disclosure (e.g., subpoena) of identifiable research data -- circumstances that generally do not pose great risk to participant privacy. Further, the scope of Certificates of Confidentiality is limited to United States-based entities. NIH should amend this Practice to specifically describe these limitations. Doing so will improve investigator and institutional awareness of how Certificates of Confidentiality work and assist in framing informed consent processes.

Comments on DRAFT Points to Consider for Designating Scientific Data for Controlled Access

COGR offers the following general comments regarding this section of the Notice:

- Importantly, the introduction to this section recognizes that one-size does not fit all in terms of controls applied to data sharing. It goes on to state that sharing without access controls may be appropriate “where participants explicitly consent to share scientific data without restrictions,” while in cases of data subject to limitations from laws, informed consent, or other sources, access controls may be a necessary means to respect those limitations. Along similar lines, researchers will need to carefully consider the repositories in which they are asked to share data, particularly repositories that were established when data sharing and management plans were less robust. We encourage NIH to consider providing additional guidance on the selection of repositories, including determination of any requirements associated with a repository, how information about data use restrictions is disseminated, and how such restrictions are enforced.
- COGR member institutions fully appreciate the need for the creation and use of controlled access data repositories in many instances. Further, we urge NIH to consider funding and operating such repositories whenever possible, as the cost of maintaining and managing controlled access will extend well beyond the end of the grant, and no other ready source

³ 45 C.F.R. §164.514(a) & (b).

⁴ 45 C.F.R. §164.514(e)(4).

of funding for such repositories is available.

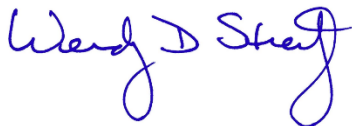
- Again, this section of the Notice references new technologies that may make data identifiable. As previously, noted, it would be of great service to the research community if NIH were to convene experts, as detailed in the 2018 Common Rule, to identify technologies/techniques that render information identifiable, along with categories of data that such technologies/techniques impact (e.g., retinal images or full-head CT scans that meet Safe Harbor de-identification standards but may be rendered identifiable via certain technologies).

Conclusion:

Agencies, institutions, and researchers must work together to promote robust sharing of data from human research participants, while ensuring that such sharing aligns with participants' expectations and is achieved in a way that protects their privacy and confidentiality. We respectfully offer our comments here as recommendations to improve the Notice's facilitation of these goals, and we appreciate NIH's solicitation and consideration of these suggestions. Finally, we also wish to take this opportunity to encourage NIH to focus on the development, establishment, and funding of additional data repositories into which shared data can be deposited, actions that will significantly assist institutions in their data sharing/management efforts.

Should you have any questions regarding this transmittal, please do not hesitate to contact Kris West, Director, Research Ethics and Compliance at kwest@cogr.edu.

Sincerely,

A handwritten signature in blue ink that reads "Wendy D. Streit". The signature is written in a cursive style with a large, looping initial "W".

Wendy D. Streit
President