

**Public Comment from the Federation of Associations in Behavioral & Brain Sciences  
(FABBS)**

Re: [NOT-OD-26-023](#) (“Request for Information on Draft NIH Controlled-Access Data Policy and Proposed Revisions to NIH Genomic Data Sharing Policy”)

Date: March 18, 2026

The Federation of Associations in Behavioral & Brain Sciences (FABBS) represents 34 of the nation’s leading scientific societies in the psychological, cognitive, and behavioral sciences. Our mission is to advance the sciences of mind, brain, and behavior; promote evidence-based policymaking; and support the integrity and impact of the federal scientific enterprise. FABBS researchers often rely on human participants to study critical public health challenges, such as maternal mortality, youth mental health, and chronic illnesses (e.g., diabetes and heart disease). Thus, we value the opportunity to comment on the National Institutes of Health’s (NIH) Draft Controlled-Access Data Policy.

We appreciate that NIH is carefully considering data security during a time of increased data sharing and collaboration between scientists. FABBS agrees with the goal of optimizing open sharing while keeping appropriate data protections in place. We have several concerns about the Controlled-Access Data Policy as it is currently proposed in this notice and want to bring attention to the potential unintended consequences of these changes.

***1. Feedback on any aspect of the Draft NIH Controlled-Access Data Policy.***

*General Concerns*

FABBS is concerned that the draft policy is too broad in scope and treats all data types identically, regardless of the privacy risks posed, which vary substantially. We encourage NIH to instead consider developing a tiered controlled-access framework that better aligns the risk proposed by certain data and the corresponding security required to minimize that risk and properly protect participant data.

In its current form, the draft policy would apply to almost all data collected from NIH-funded research that involves human participants. This policy is built on the Department of Justice (DOJ) rule concerning foreign adversaries’ access to Americans’ sensitive personal data. However, the data types covered by the policy differ widely in terms of the risks they pose and should be handled accordingly. For example, the draft policy treats “covered personal identifiers” (e.g., contact information such as address or phone number) and “personal health data” (e.g., height, weight) as identical in terms of security needed, despite the former posing

far more risk to personal privacy than the latter. Similarly, the data categories themselves are too broad, overlooking distinctions between various kinds of data within these categories. For example, “genomic data” can include whole gene sequencing or single-gene tests, which differ greatly in potential for re-identification.

The current policy does not distinguish between identified and de-identified data, a difference that has important implications for risk. In certain contexts, researchers will collect no identifying information at all. Further, even de-identified data can vary significantly in terms of potential for re-identification. As a result, the application of a single security framework to all these data types creates a mismatch between the risk posed by certain data and the security needed to minimize those risks.

Importantly, in developing this policy, NIH turned to several existing rules and standards aimed at minimizing national security threats posed by access to large-scale datasets containing sensitive information. These include the aforementioned DOJ rule (“Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern or Covered Persons” (28 CFR Part 202)) and National Institute of Standards and Technology requirements (NIST-SP-800-171). The NIST security standards are entirely appropriate and necessary when dealing with highly sensitive information that could affect our national security interests – however, few datasets coming out of NIH-funded research reach this level of risk. As such, it is ill-advised to apply the same security standards to both. Moreover, by treating all datasets as national security threats, the draft policy places considerable additional burdens on scientists conducting minimal risk research without meaningfully benefiting participant privacy, as researchers and institutions already have safeguards in place to keep these kinds of data secure (e.g., data de-identification, Institutional Review Boards often require Data Use Agreements).

Instead of a one-size-fits-all approach, FABBS encourages NIH to develop a controlled-access data policy in which security standards are proportional with the risk posed by the specific type of data. Perhaps most critically, the framework should factor in whether data are de-identified, how easy it would be to re-identify them, and how identifiable certain pieces of data are (e.g., brain images are not as identifiable as many believe them to be). We also suggest that the agency consider additional factors when aligning security and risk, including, for example: actors (i.e., who could access the data and do they pose a threat?), risk probability (i.e., how likely is it that the data will be accessed by an unsanctioned actor?), and magnitude of harm (e.g., what are the consequences of unsanctioned data access?). Such an approach would allow NIH to develop “right-sized” security frameworks – or borrow others currently in development or use elsewhere (e.g., the Research Security Program required under National Security Presidential Memorandum 33; the policies used by the Inter-University Consortium for Political and Social Research (ICPSR) and OpenNeuro) – that are better suited for academic research data.

### *Potential Unintended Consequences*

FABBS is also concerned about potential unintended consequences of the draft Controlled-Access Data Policy. Before moving forward with revisions or implementation, we urge NIH to conduct a thorough assessment of potential consequences and how to mitigate them. Especially for minimal risk research involving de-identified data, the potential drawbacks outweigh the potential (limited) benefits to participant protection and privacy.

By way of example, the recent NIH decision to eliminate Basic Experimental Studies Involving Humans (BESH) from the definition of clinical trials reveals the value of doing such a pre-implementation assessment. In 2014, the agency redefined clinical trials to include basic behavioral and social science research. As a result, scientists in these fields had to comply with registration and reporting requirements designed for clinical trials rather than tailored for basic discovery research. This proved to be untenable leading NIH to attempt to remedy the problem with a new classification, but this was still unworkable. Twelve years later, NIH reversed course and will no longer consider BESH to be clinical trials. An initial, more thorough consideration of the possible unintended consequences of changing the clinical trials definition may have saved the agency and researchers from substantial confusion, time, and effort.

The following list of potential consequences is not exhaustive.

- As currently proposed, the draft policy would significantly increase the number of studies requiring controlled-access security. In turn, this would stretch the capacity of the current repository infrastructure as well as increase compliance and administrative burdens on scientists, with little if any benefit to participant privacy.
  - At this time, repository infrastructure is inadequate for handling the expansion of data types requiring controlled access that will occur if the draft policy is implemented. Improving this infrastructure will be difficult due to the required costs and resources, which may be prohibitive to many researchers and institutions. To develop compliant repositories, researchers and/or institutions must have the funds to cover, for example, technology investments, ongoing compliance monitoring, personnel training, and regular security audits. (The NIT-SP-800-171 standards cited in the policy require 110 distinct security controls, formal system security plans, and regular assessment.)
    - Certain institutions – in particular R2 institutions and other Research Colleges and Universities (RCUs), including community colleges – may not have the resources to make or keep repositories compliant. Even the most well-resourced R1 institutions may have trouble funding compliance activities, but they will still have an advantage over smaller, less-resourced institutions in developing and maintaining repositories. As a result, this policy may exacerbate the gap in funding and research output between R1s and other research institutions, especially those that, historically, have been underfunded.

- The costs involved may also force researchers to recruit smaller samples than originally intended, resulting in less reliable findings due to lower statistical power.
  - In other new policies (e.g., limiting allowable publishing costs), NIH has committed to maximizing the amount of grant funds actually spent on research versus administrative and other costs. The draft Controlled-Access Data Policy, however, will likely further divert funding from research activities to data security and compliance activities as, noted above, individual researchers and institutions may not have the resources to fund these themselves.
    - Recognizing the time and resources necessary to comply with these new standards, the policy risks diverting scientists' time away from research itself.
- There is a risk that the draft policy could slow secondary data analysis by increasing the barriers to data access for many researchers. Secondary data analysis efforts include meta-analyses, reproducibility efforts, and replication studies, the latter two of which are critical to Director Dr. Jay Bhattacharya's vision for the NIH. Limiting secondary data-analyses would further undermine confidence in scientific findings.
  - As noted above, the stricter requirements on data repositories required by the draft policy would limit accessibility to data, especially for researchers from lesser-resourced institutions. The ability to do data analysis and share data may be further centralized to a few well-resourced institutions that can afford to stay in compliance.
  - Researchers-in-training and early career scientists may be uniquely impacted due to their reliance on existing datasets in their work and training.
  - The new requirements may also discourage researchers from making their data available to other scientists or may lead them to design studies in ways that avoid overly burdensome compliance activities.
    - Large-scale data sharing is critical to understanding many health problems, including those intractable disorders that have substantial human and economic impact (e.g., neurological and autoimmune conditions). Reducing or even disincentivizing data sharing will significantly harm our ability to develop cures and treatments.

FABBS is grateful for NIH's work on this issue as well as the opportunity to share our feedback. We are happy to serve as a resource to NIH as it continues to develop this policy.