March 18, 2026
National Institutes of Health
Office of the Director
9000 Rockville Pike
Bethesda, MD 20892

Re: Response to RFI NOT-OD-26-023 — Draft NIH Controlled-Access Data Policy and Proposed Revisions to the NIH Genomic Data Sharing Policy

Dear:
On behalf of the American Medical Informatics Association (AMIA), we appreciate the opportunity to respond to RFI NOT-OD-26-023 regarding the Draft NIH Controlled-Access Data Policy and proposed revisions to the NIH Genomic Data Sharing (GDS) Policy. AMIA represents more than 6,000 biomedical and health informatics professionals who develop, implement, and evaluate the data standards, governance frameworks, and analytic systems that underpin modern biomedical discovery and clinical care.

AMIA supports NIH's efforts to modernize and harmonize its data governance framework in light of rapid technological advancement, expanding data linkage capabilities, and evolving privacy and national security considerations. Across both policies, we encourage NIH to adopt a proportionate, risk-based, and harmonized approach that advances scientific utility while safeguarding participant trust, supported by sustained infrastructure investment and equitable implementation.

NIH Controlled-Access Data Policy

AMIA supports NIH's objective of clarifying when human participant data warrant controlled access rather than open dissemination. We offer the following key recommendations to strengthen the policy:

1. Adopt a proportionate, risk-based framework

AMIA urges NIH to move beyond categorical designations based solely on data type and instead adopt a flexible, risk-based model. Re-identification risk increasingly depends on context, linkage potential, and analytic capability, particularly in multi-modal environments that combine genomic, clinical, imaging, and social determinants data.[1] A framework that

accounts for contextual risk, technical safeguards, and intended scientific use would better balance participant protection with scientific utility.

2. Ensure harmonization across NIH data policies

NIH should align the Controlled-Access Data Policy with the Data Management and Sharing (DMS) Policy and the revised GDS Policy. Fragmented implementation across Institutes and Centers creates unnecessary complexity. Clear guidance should explain how controlled-access determinations intersect with DMS Plans, repository selection, and informed consent expectations, improving compliance while reducing administrative burden.[2]

3. Invest in infrastructure, governance, and workforce capacity

Effective controlled access depends on robust repository ecosystems. Consistent with prior AMIA recommendations, policy mandates must be paired with sustained support for infrastructure and workforce development.[3] NIH should:

- Define minimum technical, governance, and cybersecurity standards for controlled-access repositories;
- Provide sustained funding for data stewardship, auditing, and access review;
- Support workforce development for biomedical data stewards and informatics professionals; and
- Ensure interoperability across NIH-funded repositories.

4. Implement flexible, risk-aligned security requirements

While AMIA supports strong data protections, applying uniform and prescriptive standards, such as broad application of NIST SP 800-171A, risks creating unintended disparities.[4] Under-resourced institutions, including community-based organizations and emerging research programs, may face significant barriers to compliance, limiting participation and exacerbating inequities.

Moreover, applying such requirements only to NIH-funded datasets creates a fragmented security landscape that may not meaningfully advance national privacy or security goals. NIH should instead adopt a flexible, risk-based security framework aligned with data sensitivity and use, coupled with implementation support to ensure broad participation.

5. Clarify alignment with existing regulatory frameworks

NIH should provide clear guidance on how controlled-access requirements interact with existing regulations, particularly the HIPAA Privacy and Security Rules.[5,6] In many cases, HIPAA already establishes robust protections for human participant data. Duplicative or misaligned requirements risk increasing administrative burden without improving security

outcomes. Greater clarity will reduce compliance complexity and support efficient data sharing.

Genomic Data Sharing (GDS) Policy

AMIA supports NIH's efforts to harmonize the GDS Policy with the broader DMS framework. To strengthen implementation, we recommend:

1. Address governance of multi-modal and linked datasets
Genomic data are increasingly integrated with phenotypic, environmental, and real-world data sources.[1] NIH should explicitly address governance for linked and derived datasets, including privacy-preserving linkage methods and secure analytic approaches such as federated and enclave-based models.

2. Strengthen participant trust through transparent data stewardship
Participant trust is foundational to data sharing. NIH should provide model consent language adaptable to evolving research contexts, clarify expectations for legacy datasets, and promote transparency mechanisms that inform participants about downstream data use and governance safeguards.[1,3]

3. Promote equity in access and participation
Controlled-access processes that are overly complex, costly, or time-consuming risk disadvantaging early-career investigators, community-engaged researchers, and under-resourced institutions. NIH should assess approval timelines, administrative burden, and repository access costs to ensure equitable access to publicly funded data resources.[1]

4. Preserve responsible international collaboration
Genomic research relies on global infrastructure and partnerships. Restrictions that limit the use of international platforms or resources could hinder scientific progress and reduce the competitiveness of U.S.-led research. NIH should ensure policies enable responsible international collaboration while maintaining appropriate safeguards.

Artificial Intelligence and Reproducibility

As controlled-access environments increasingly support artificial intelligence (AI) and advanced analytics, NIH policies should explicitly enable reproducible and secure AI development. AMIA has emphasized the importance of interoperable standards, reproducibility, and responsible AI integration within biomedical research ecosystems.[3]

NIH should clarify whether secure computational access models, such as data enclaves and federated analysis, satisfy policy requirements and support consistent reproducibility standards in controlled-access environments.

***

AMIA commends NIH for proactively refining its data governance policies to address emerging scientific, ethical, and security considerations. We strongly support a harmonized, risk-based framework that balances participant protection with scientific utility, aligns requirements across NIH policies and existing regulations, invests in sustainable infrastructure and workforce capacity, and promotes equity, innovation, and global collaboration. AMIA stands ready to serve as a technical partner as NIH refines and implements these policies. For more information, please contact AMIA's Senior Manager of Public Policy, Tayler Williams, at twilliams@amia.org.

Sincerely,

Eileen Koski

Eileen Koski
Chair, AMIA Public Policy Committee

References

1. American Medical Informatics Association. *AMIA Response to NIH NLM Extramural Research Programs RFI (NOT-LM-25-002)* (2025), AMIA-Response-NIH-NLM-Extramural-Programs-RFI.pdf.
2. American Medical Informatics Association. *AMIA Comments on NIH Data Management and Sharing Policy Proposals* (2018–2020), AMIA-Supports-New-NIH-Data-Policy-Encourages-Phased-Implementation.pdf.
3. American Medical Informatics Association. *AMIA Response to NIH Strategic Plan for Data Science 2023–2028 RFI* (2024), AMIA-NIH-RFI-Strategic-Plan-for-Data-Science-2023_2028.pdf.
4. National Institute of Standards and Technology. *Assessing Security Requirements for Controlled Unclassified Information*. NIST Special Publication 800-171A Rev. 3, (2024), https://doi.org/10.6028/NIST.SP.800-171Ar3.
5. U.S. Department of Health & Human Services. HIPAA Security Rule: Laws and Regulations. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
6. U.S. Department of Health & Human Services. HIPAA Privacy Rule: Laws and Regulations. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.