Comments of the World Privacy Forum

To

National Institutes of Health

Regarding Request for Public Comments on a DRAFT NIH Policy for Data Management and Sharing and Supplemental DRAFT Guidance

Comments submitted via: https://osp.od.nih.gov/draft-data-sharing-and-management

Andrea Jackson-Dipina, Dr.PH
Director of the Division of Scientific Data Sharing Policy
Office of Science Policy, NIH, 6705 Rockledge Drive
Suite 750
Bethesda, MD 20892

December 18, 2019

The World Privacy Forum is pleased to have the opportunity respond to the request of the National Institutes of Health for public comments on a draft NIH policy for data management and sharing and supplemental draft guidance. The request appeared in the Federal Register on November 8, 2019, 84 Fed. Reg. 60398, https://www.federalregister.gov/documents/2019/11/08/2019-24529/request-for-public-comments-on-a-draft-nih-policy-for-data-management-and-sharing-and-supplemental.

The World Privacy Forum is a nonprofit, non-partisan 501(c)(3) public interest research group. The WPF focuses on privacy, with health privacy among our central focuses. We publish and maintain a large body of health privacy work, including a patient's guide to HIPAA, reports on and FAQs for victims of medical identity theft; and reports on genetic privacy, precision medicine, electronic health records, and other topics. We regularly testify before Congress and federal agencies, and we submit comments on HIPAA and other regulations with relevance to privacy and security. More about our work and our reports, data visualizations, testimony, consumer guides, and public comments can be found at http://www.worldprivacyforum.org.

The World Privacy Forum supports the broad goals of the draft policy. Responsible research and the appropriate sharing of research data are worthy objectives. Our comments address the policy as it relates to the privacy and security of data about human subjects.

We preface our suggestions with a few observations about researchers. While there are many responsible researchers, we find that too many researchers want everyone's data but are unwilling to accept or implement the level of responsibility required to provide meaningful privacy and security for this personal data. At present, we must accept the Institutional Review Board process as it is today. However, we also note there are meaningful gaps in protections even when institutional review boards oversee research activities.

Privacy and security are only sometimes adequately addressed in the IRB process because only some IRBs have the knowledge, motivation, and interest to require that research projects maintain proper privacy and security protections. A factor in this difficulty is that IRB members only occasionally have the needed expertise in privacy or security. We recognize that this is not the place to address generally the shortcomings of the IRB process. We also recognize that the IRB process is an area that would benefit from increased policy attention, particularly as it relates to human subject research, including research that is incorporating AI and machine learning aspects.

Some cities are undertaking innovative work on IRBs, for example, Columbus, OH has a community IRB process. See: https://orrp.osu.edu/irb/research-participants/community-engaged-research/. The city of Cambridge, MA has an open data review board, https://data.cambridgema.gov/General-Government/Cambridge-Open-Data-Ordinance-092115/tf4d-q3qs. We hope that the smaller efforts seeking to update IRB processes will continue, and will spark larger scale projects updating IRBs.

In the meantime, the point is that no one can assume that existing mechanisms (like IRBs) or that the researchers themselves can guarantee suitable protections for privacy and security. Thus, casual references to privacy and security in a summary list of requirements for data management and sharing in the guidance is not likely to make a meaningful difference. Much health research data in the hands of researchers is not subject to the privacy or security rules in HIPAA. **Indeed, most research data about individuals is not subject to any existing privacy law in the United States**. This contrasts with the situation in the European Union and much of the rest of the world, where researchers are generally be subject to the same data protection rules as others who process personal data.

NIH is one of the few institutions that has the clout to impose more specific privacy and security obligations on researchers. We do not suggest, however, that NIH use the proposed guidance to promulgate privacy and security regulations on those who receive NIH funding. Still, NIH can do better than a few casual references to privacy and security.

For example, we suggest that guidance include specific references to current NIST security guidance and to HIPAA security standards. Telling researchers that they must address security is one thing. Telling researchers that their security measures must be as rigorous as those from specifically identified and generally authoritative sources is more likely to be noticed and to

result in a reasonable level of security. We observe that the supplementary information for the draft guidance includes a specific reference to several NIH genome policy documents and to other NIH policy materials. We suggest something similar here. More references to appropriate security documents – especially ones that the authors of those documents keep up to date – would make the guidelines more useful to data users and more beneficial to data subjects. Referencing standards would also help during project evaluation.

We make the same suggestions for privacy. NIH documents and standards like the Common Rule are filled with vague and general references to privacy and confidentiality in research. All lack meaningful standards to tell researchers what they should do. Recent revisions to the Common Rule failed to include the more specific privacy and security obligations for researchers that the draft rule proposed. NIH should point to specific privacy policies used in existing research as models for everyone to follow. Telling researchers that research projects will be evaluated by NIH in part on the basis of specific privacy and security standards has the potential to make a difference.

We make the same suggestion yet again for data de-identification obligations. Numerous organizations maintain best practices for data de-identification. NIH should select several as examples, choosing those where the authors keep the documents up to date. De-identification is a much more prominent legislative issue now at the state level in the US and globally. We expect that researchers need to be much more aware going forward about what the proper standards are for de-identification in various research contexts. We note that privacy-related laws drafted or passed the last few years introduced more precise language and requirements around de-identification. See, for example, various state level laws in the US, including the CCPA, and see for example, the GDPR in Europe, and most recently, India's Data Protection Bill 2019.

Where the NIH draft guidance addresses data sharing agreements, we think that providing references to sample agreements would be valuable. Providing a wide range of models would be much more effective than a vague admonition to do *something* appropriate with respect to privacy and security.

Further, we suggest that NIH require – or at the very least, suggest – that all data sharing agreements expressly include language stating that data subjects are third party beneficiaries of the agreement. Unless data subjects have the ability to enforce the privacy and security requirements of a data sharing agreement when and if the need arises, violations of an agreement will never be pursued because the parties to the agreement will likely have no interest in doing so. We do not suggest a third-party beneficiary clause as a cure-all, but it will offer a possible enforcement tool that would otherwise be absent.

In closing, we appreciate that NIH's draft guidance focuses on the importance of privacy and security in data sharing. We observe, however, that the draft's reference to protective measures "that are consistent with applicable federal, tribal, state, and local laws, regulations, statues [sic], guidance, and institutional policies" has little meaning as the research world largely falls outside of any privacy and security rules in the US.

Further, even this broad suggestion to comply with "applicable" rules is inadequate. Much research is international in scope/ The conduct of research and the international transfer and location of research data about individuals implicates data protection rules in other countries. Nearly every other country in the world has generally applicable data protection rules, and the United States is the only major outlier. NIH should use its guidance to tell U.S. researchers that they need to be aware of the consequences of international activities.

NIH still has a narrow band of time in which it can be proactive regarding privacy, noting that privacy legislation is under active consideration in the Congress and in other countries as well. To proactively address privacy issues, NIH needs to do more than it proposes in its guidance to properly advise the research community and to protect data subjects.

Incorporating more specific and relevant guidance is an important starting point. We are only a front-page scandal away from the imposition of new state and federal laws that would provide the type of privacy and security protections now lacking in the research world in the US. NIH needs to step up and do its part to provide more meaningful and more useful guidance for the research community before someone else does. The health sector, including the kinds of research the NIH draft guidance seeks to address, is enormously complex. Legislation can sometimes be a blunt tool that does not acknowledge those complexities. We urge NIH to be as proactive as possible in its guidance.

Thank you for the opportunity to comment on the draft guidance.

Respectfully submitted,

s/

Pam Dixon
Executive Director, World Privacy Forum
www.worldprivacyforum.org
3 Monroe Parkway, Suite P #148
Lake Oswego, OR 97035