America's Oldest National Monthly IRB Newsletter

Human Research Report™

PROTECTING RESEARCHERS AND RESEARCH SUBJECTS

Volume 37, No. 6 ISSN 0885-0615 June, 2022

IRBs and Protecting the Privacy of Human Research Subject Data

The National Institutes of Health (NIH) is now launching a major effort to update an area that often tasks IRBs; namely, the privacy of human research subjects and the confidentiality of their research data.

This is especially a problem due to the current NIH requirements on data-sharing and public access to research data.

> "NIH is seeking public comments on draft supplemental information in the *NIH Policy for Data Management and Sharing* to address privacy considerations.
>
> This information is not intended to provide a guide for compliance with regulatory requirements, but is rather 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*" ("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*," Notice Number NOT-OD-22-131, May 12; at https://grants.nih.gov/grants/guide/notice-files/NOT-OD-22-131.html).

Three Areas of Concentration for Privacy

NIH plans to release a final version of their recommendations later this year.

> "Effective data stewardship and protection of human research participant … privacy are achieved in tandem through responsible scientific data sharing practices.
>
> Accordingly, NIH has developed supplemental information to the *NIH Policy for Data Management and Sharing* … to assist stakeholders in achieving this goal by establishing 1) operational principles for protecting participants' privacy when sharing scientific data, 2) best practices for implementing these principles, and 3) points to consider for designating scientific data for controlled access" (supra in "Background" section).

While we refer our HRR readers to the original source NIH document for full details, we present below some samples of each of the three areas

NOTE #1: Quoted materials in this newsletter appear exactly as originally published in source documents, including any misspellings, grammatical errors, or missing words. However, we will on occasion insert words or edit text and/or formating in brackets [ ] to make the material easier to read.

NOTE #2: Emphases are added to articles by HRR by underlining or adding ***bold/italics*** to selected text, unless stated otherwise.

NOTE #3: Articles **To Be Continued** in subsequent issues are marked at the end of the article with **{TBC}**.

Also In This Issue

Published monthly by The Deem Corporation, P.O. Box 451117, Omaha, NE 68145. Editor and Publisher: Dennis M. Maloney, Ph.D.

listed above to facilitate HRR reader judgments on which area might be most relevant for any particular IRB.

We begin with the area of "operational principles for protecting participant privacy."

> "**1.** NIH and the institutions it funds are obligated and required to protect the privacy and confidentiality of every participant as described in informed consent and in line with all applicable laws, policies, and regulations" (supra in section titled "DRAFT Operational Principles for Protecting …").

"De-Identified" Is Not Automatic Privacy Protection for Subjects

> "**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).
>
> **3.** Investigators and institutions should develop robust consent processes that prioritize clarity regarding future sharing and use of scientific data ….
>
> 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" (ibid).

Legal Protections Include "Certificates of Confidentiality"

There are three subsections in the second main area of "best practices." Those subsections are titled "Ensure Appropriate De-identification," "Establish Scientific Data Sharing and Use Agreements," and "Understand Legal Protections Against Disclosure and Misuse."

We present here the brief third subsection, as follows:

> "Per the *NIH Certificates of Confidentiality Policy*, data subject to the Policy are deemed [to be] issued a Certificate of Confidentiality, including some data that have been de-identified (e.g., human genome 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" (supra in subsection "Understand Legal …").

"Controlled Access Repositories" Can Be Key

Finally, for the third subsection titled "DRAFT Points to Consider …", we present:

> "The DMS Policy expects researchers to consider whether access to scientific data from participants should be controlled (i.e., measures such as requiring data requesters to verify their identity and the appropriateness of their proposed research use to access protected data), even if de-identified and lacking explicit limitations on subsequent use.
>
> The points below are intended to assist researchers when considering whether controlled access repositories may be needed to protect participant privacy.
>
> Note that controls may be needed for data at any level of processing (e.g., raw or fully cleaned data) and from any source (e.g., research, clinical, or public health data) …."

"Controlled Access" Has Its Own Requirements

> "Investigators should consider sharing participants' scientific data through controlled access repositories if data:
>
> **1.** Have explicit limitations on subsequent use, such as those imposed by laws, regulations, policies, informed consent, and/or agreements ….
>
> **3.** Cannot be de-identified to established standards or cannot sufficiently reduce the possibility of re-identification."

Comments are due by June 27. For more information, contact: NIH Office of Science Policy at SciencePolicy@od.nih.gov. © **{TBC}**