General JHU IRB Expectations for Sharing of Individual Level Research Data *

Data Sharing is increasingly common and may be required for funded research or for publication purposes. The table below outlines considerations researchers should be aware of when developing plans for data sharing when the data to be shared is from human research participants. The first column identifies common sharing formats, the second column sets forth possible consenting scenarios and the third column outlines considerations researchers should be prepared to address in any data sharing plan.

Sharing Format	Consent	Other Considerations
Open Access	Explicit Consent for sharing via Open Access is obtained.	• Open Access sharing must be consistent with applicable laws, local approvals and governing agreements (funding, MTAs, DUAs, etc.) • Sharing must not pose greater than minimal risk to individual participants or communities/groups • Explicit consent for sharing via open access is required and the consent must specify the type of data and identifiability of the data to be shared
Controlled Access	Where Explicit Consent for sharing via Controlled Access is obtained	• Controlled Access sharing must be consistent with applicable laws, local approvals and governing agreements • Sharing must not pose greater than minimal risk to individual participants or communities/groups • Consent must specify the type of data and identifiability of the data to be shared • The level of controls required may vary based on the sensitivity of the data and likelihood of re-identification
	Consent obtained prior to January 25, 2023 without explicit sharing language, and does not prohibit sharing	• Sharing via controlled access must be consistent with any applicable laws, local approvals and governing agreements • Sharing must not pose greater than minimal risk to individual participants or communities/groups • The level of controls required may vary based on the sensitivity of the data and likelihood of re-identification • Only datasets without direct identifiers (limited data sets or de-identified data sets) may be shared
	Data obtained under an IRB approved waiver of consent,	• Sharing via controlled access must be consistent with any applicable laws, local approvals and governing agreements • Sharing must not pose greater than minimal risk to individual participants or communities/groups • The level of controls required may vary based on the sensitivity of the data and likelihood of re-identification • Only completely de-identified data sets as determined by an honest broker may be shared ** ** JHU IRBS may consider exceptions with exceptional controls, such as a secure enclave (consider identifying standards and examples)

*The JHU IRBs may consider exceptions to the above guidelines on a case by case basis.

DEFINITIONS

Open Access: Open access data sharing allows anyone to access and use the dataset. For the data to be made publicly available, all information, both direct and indirect, that could lead to a person being identified must be removed. (For healthcare data this is called de-identification when conformant with HIPAA standards). Datasets from rare disease communities require the removal of more information than for more common disease communities to safely protect a person's identity. Although necessary, this level of de-identification of data can limit the usefulness of the dataset.

Controlled Access: Controlled access data sharing requires a request for access to the dataset to be approved. The requirements vary, but usually limit data sharing to researchers with a specific, relevant research question. Data sharing restrictions are determined by the owner of the data prior to collection of the data and for consented studies are should be described in the informed consent . A Data Sharing Agreement and/or Data Use Agreement are often used in controlled access data sharing. Although the information that may directly identify a person must be removed, the amount of information to be removed may vary based on risk and level of controls.

Restricted Access: Data cannot be shared or released directly to the public research community due to possible risk(s) to study participants as well as to protect the data confidentiality promised to them.

Minimal Risk: Minimal risk means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life of the general population or during the performance of routine physical or psychological examinations or tests.