SAMPLE DATA USAGE AGREEMENT

This is intended to be used to guide an individual in using procedures and language for describing the lifecycle of Level 3 confidential research data, as outlined at https://security.harvard.edu/dct. Although Level 3 data can be stored and manipulated on local computers that meet both HBS IT and HU IT security guidelines, this document makes the assumption that all work will be conducted on the HBS Compute Grid.

What information is being collected?

(this is determined by the research team)

Who has access to the data?

(this is determined by the research team)

How is the data being transferred?

Sensitive data will be transferred either by HBS secure file transfer service (a web application from Accellion, Inc.) or by a method of the data originator's choice. Note that it is against Harvard University regulations to use a service that does not provide encryption in some form, unless the data is already encrypted before transit.

Where and how will the data be stored?

The sensitive data will be stored on the storage arrays as a part of the HBS Compute Grid infrastructure, which has been certified to house both Level 3 and Level 4 data. Access to project areas for all sensitive information levels are audited and restricted by Unix POSIX permissions, and is neither visible nor accessible to users other than the project members. The project team can further de-identify the data, if possible, permitting its use beyond the compute grid, and the identifying information will be encrypted and remain in the L3 project team directory.

How should the data be analyzed and/or manipulated?

In its Level 3 state, the data will be manipulated and analyzed *in situ* on the HBS compute grid.

What is the backup policy?

The storage arrays as part of the Level 3 and Level 4 setup are backed up on a nightly basis, also in an confidential information-approved environment. The data provider can request that the data in one or more forms (e.g. raw, partial, analyzed, etc) be excluded from backups.

What is the retention policy?

Data will be retained per agreement between the research team and the data provider. Usually this is through the time of publication, and three years beyond in order to allow for the research team to conduct any remedial corrections or analysis post-publication.

How will the information be discarded?

The researcher or HBS IT staff can assist in discarding data via a secure-erase method (if needed), as directed by the data provider.