CITF Data Security Policy

1. **Encryption and Password Protection.** Researchers agree that the CITF Data will be stored primarily on password-protected desktop computers or servers. If stored on mobile devices, such as laptop computers or remote storage devices, the CITF Data will remain encrypted when at rest.
2. **Physical Safeguards.** Researchers agree to keep desktop computers and servers holding the CITF Data in private rooms that can be locked and to lock the doors thereof if the researchers are not on site to monitor the use of the CITF Data.
3. **Data Safeguards.** Researchers agree to use a recognized virus and malware protection software on the desktop computers, laptop computers or remote storage devices (provided these can be outfitted with such protection) that will host the CITF Data.
4. **Organizational Safeguards.** Researchers agree to implement and adhere to organizational practices that enhance data security. Access to data must be limited to authorized personnel. Authorized personnel must remain demonstrably accountable to institutional leadership and senior personnel, as well as to the institution itself.
5. **Data Destruction.** Researchers agree to destroy the CITF Data at the time determined in the Data Request Form or equivalent document. Researchers agree to use an auditable method of data destruction to destroy the CITF Data. Researchers agree to maintain documentation evidencing the destruction of the CITF Data and to make such records available to the CITF on request.
6. **Training.** Researchers agree to ensure that the principal investigator, authorized personnel, authorized students and other persons at their institution that access the CITF Data are provided with training that addresses data security and data privacy, to a degree that is appropriate to their role and responsibilities.
7. **Record-keeping.** Researchers agree to maintain records of who has access to the CITF Data under their control or in their possession. Researchers agree to record the time interval and scope of data elements accessible to each approved user. Records must also be maintained detailing data destruction.
8. **Monitoring and Audit.** Records regarding CITF Data access and destruction shall be stored using technological means that allow for audit internally and by external researchers. Audits of user activity shall be conducted on a regular basis and shall be conducted immediately when irregular user activity occurs.
9. **Data Breaches.** Researchers shall use industry-standard technological mechanisms appropriate to protect health data to prevent data breaches, and that allow for data breaches to be detected. If a data breach occurs that is known or suspected to affect CITF Data, the CITF must be informed immediately and all known information about the data breach must be provided to them.
10. **Vulnerability Management**. Researchers agree to immediately take measures to patch and/or remediate all software and other security vulnerabilities that are discovered which could affect the CITF Data. Researchers agree to have policies in place to ensure the prompt and ongoing patching of vulnerabilities and to implement that policy effectively.
11. **Third Party Service Providers**. Researchers agree to use all contractual and other measures necessary to ensure that Third Party Service Providers comply with the terms of this Policy and are demonstrably held accountable to the CITF.

12. **Cloud Storage and Cloud Computing**. Researchers agree to adopt all contractual and other measures necessary to ensure that all Cloud Storage and Cloud Computing providers that will use or access the CITF Data remain accountable to them and to the CITF. These measures shall include, but not be limited to, providing specific details as to, and guaranteeing the auditability of: the jurisdictions of storage of the CITF Data, data retention and destruction practices, segregation of the CITF Data from other data, implementation of appropriate security measures, maintenance of adequate access logs, and adoption of appropriate procedures for resisting compelled access to the CITF Data.