Resource for Genetic and Epidemiological Research
Standard Data Security Assurances

For all data approved by Resource for Genetic and Epidemiological Research (RGE), including data from the Utah Population Database, Utah Cancer Registry, and all data contributors, the Principal Investigator will:

1. Maintain a current list of all personnel with access to data approved by RGE for this project and submit an updated list of such personnel to RGE whenever a change is made and with the project annual renewal.

2. Require that all personnel with access to data approved by RGE for this project complete human subjects research training, privacy and information security training, and sign and submit RGE Confidentiality Agreements.

3. The number of users of the data, particularly those authorized to access data approved by RGE for this project, will be kept to the minimum necessary to accomplish the project.

4. For each user of the data, the Principal Investigator will authorize a unique user name and password which allows access only to files and records for which the user has been approved.

5. Ensure that data access is revoked for personnel no longer working on this project.

6. Inform RGE in writing of any changes in the administrative responsibility or the physical location of the computer(s) on which data approved by RGE for this study is stored.

7. House computers, data files, remote terminals, computer tapes and printers in a secured facility (locked rooms accessible only by authorized personnel).

8. Data may be stored on servers and laptops or other portable media and storage devices (such as CDs, DVDs, flash drives, external hard drives, etc.) ONLY IF SUCH DEVICES ARE ENCRYPTED.

9. Data may be transmitted electronically only if encrypted during transmission.

10. Ensure that adequate safeguards against malicious software are installed on all computers housing data approved by RGE for this project (ie. anti-virus software, malware protection, and all critical operating system updates).

11. Report any suspected or known security breach of data approved by RGE within 24 hours.

12. Submit to unannounced audits of data approved by RGE stored on project computers.

13. All identifying information stored electronically will be kept separate from other project information.

14. ID numbers will replace identifying information when labeling specimens for laboratory work and for the use of protected data by collaborators at other institutions.

15. Researcher will not disclose the RGE approved data except as expressly authorized by RGE approval of this application for data use. Obtain permission from RGE by submitting a revised or new proposal before transferring any data approved by RGE outside of the performance site(s) listed on page one of this application.

Any exceptions to these standard assurances must be reviewed and approved by RGE. Please submit a detailed written description of the circumstances and reasons for requesting any exception(s).

As Principal Investigator, I have read and agree to the RGE Standard Data Security Assurances.

_____ _____

Signature Date

Name: _____

(Please print)

Title: _____

Institution _____