RGE Standard Data Security Assurances

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).

For all electronic and printed data obtained through RGE approval (RGE data), the Responsible/Principal Investigator will:

1. Maintain a current list of all personnel with access to RGE data for this project and submit an updated list of such personnel to RGE in ERICA whenever a change is made and with the project annual renewal.
2. Require that all personnel with access to RGE data for this project sign and submit a current RGE Confidentiality and Data Use Agreement and complete data privacy and information security training for human subjects research.
3. Keep the number of users of the data, particularly those authorized to use individually identifying information, to the minimum necessary to accomplish the project.
4. Ensure that each user with electronic access to RGE data is assigned a unique username and password which allows access only to the RGE data for which the user has been approved.
5. Ensure that access to RGE data is revoked for personnel no longer working on this project.
6. Amend the ERICA RGE application prior to making changes in the administrative responsibility or the physical location (s) of the computer(s) housing RGE data.
7. House electronic RGE data ONLY in the data storage location(s) approved by RGE in the ERICA RGE application.
8. House printed RGE data in a secured facility (locked cabinets or rooms accessible only by authorized personnel) in the study location(s) listed in the ERICA RGE application.
9. Ensure that adequate safeguards against malicious software are installed on all computers housing UPDB data (i.e., anti-virus software, malware protection, and all critical operating system updates).
10. Report any suspected or known security breach of data to RGE within 24 hours.
11. Submit to unannounced audits of data storage location(s) and data security procedures.
12. Separate all identifying information stored electronically from other project information.
13. Replace identifying information with ID numbers when labeling specimens for laboratory work and for the use of RGE data by collaborators at other institutions.
14. Obtain permission from RGE before transferring any electronic or printed RGE data outside of the study location(s) listed in the ERICA RGE application.
15. Dispose of electronic and printed RGE data at the end of the project and submit a Certificate of Data Disposition to RGE.

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

_____

Signature Date

Electronic signatures are available through DocuSign. Please contact the RGE Office at rge@utah.edu for electronic signing instructions.