University of La Verne Institutional Review Board
Policy and Procedure on Data Protection
Approved: May 11, 2018,
Amended May 23, 2018, September 19, 2018

Policy:

1. **Non-HIPAA Data**
   Data and informed consents collected for IRB-approved research are subject to the highest security possible. Thus, applicants are required to store data in any of the following venues:

   a. Paper forms: locked in a University of La Verne filing cabinet, also locked in a University of La Verne office
   b. Paper forms: locked in a stationary cabinet in researcher's non-University of La Verne office
   c. A password-protected computer stored in a locked University of La Verne office
   d. A password-protected computer that only the researcher can access, stored in a locked non-University of La Verne Office
   e. A password-protected drive or similar storage device locked in a University of La Verne filing cabinet, also locked in a University of La Verne office
   f. The applicant's University of La Verne email (Google Gmail for students, Outlook for faculty/staff/administration)
   g. The University of La Verne's provided OneDrive (other OneDrives are not accepted)
   h. The University of La Verne's provided Qualtrics
   i. The University of La Verne's provided GoogleDrive (other GoogleDrives are not accepted unless they fall under (i) below)
   j. Dropbox Education or Dropbox Business (evidence of such a subscription is required to be provided during application review)
   k. Any other cloud storage that is demonstrated to be FERPA and GDPR compliant (e.g., a signed contract and evidence of purchase of the appropriate cloud storage package, a signed contract with the data provider showing the desktop requirements have been met, etc.) or non-electronic equivalent with proper documentation of its adequate protections

2. **For data that fall under HIPAA:**

   a. Paper forms: locked in a University of La Verne filing cabinet, also locked in a University of La Verne office
   b. A HIPAA compliant cloud storage system, desktop equivalent, or non-electronic equivalent with documentation the storage is HIPAA and GDPR complaint (e.g., a signed contract and evidence of purchase of the appropriate cloud storage package, a signed contract with the data provider showing the desktop requirements have been met, etc.)

Procedures:

Applicant will select storage procedure in application from the lists above. If any documentation is needed by the policy, applicant will upload documentation to application.

i. IRB Analyst will verify data storage protocol described in the application and if options 1(i) or 2(b) are invoked, the Analyst will verify appropriate documentation is attached.
ii. Lead and Second Reviewers will review storage selection and documentation (if applicable) to verify the data storage solution provides adequate protections for the type of data being stored
iii. Chair will also review storage selection and documentation (if applicable) to verify the data storage solution provides adequate protections for the type of data being stored
    a. If documentation is inadequate, the Chair will send the application back to obtain suitable documentation/storage selection
iv. Once appropriate storage has been selected and adequate documentation (if required) received and reviewed, the Chair will proceed with making a determination on the application