TEACHERS COLLEGE
COLUMBIA UNIVERSITY
Institutional Review Board
Box 151 | 525 West 120th St. New York, NY 10027
212-678-4105 | RH 13 | IRB@tc.edu | tc.edu/IRB

BEST PRACTICES FOR SECURING RESEARCH DATA ACROSS TEACHERS COLLEGE, COLUMBIA UNIVERSITY

Information Security Standard Procedures & Policies

INTRODUCTION

Best practices for securing research data should be used for ALL data collected or received electronically by Teachers College (TC) researchers. Researchers are required to justify research projects involving sensitive data that depart from or omit the procedures listed below on the Institutional Review Board (IRB) application. The Principal Investigator (PI) is responsible for securing collected, stored, transmitted, or shared data. The PI is also responsible for training research staff on transmitting, securing, and safeguarding research data.

SECURING RESEARCH DATA

- □ Ensure that all of your computing devices are encrypted and have antivirus software installed. TC-issued laptops are automatically encrypted and have antivirus software installed. Contact the TC Information Technology (TCIT) Service Desk for assistance (servicedesk@tc.columbia.edu).

- □ Follow "Minimum Necessary" guidelines. Only allow those who need the data the minimum access necessary to complete their task.

- □ Only authorized research staff can have access to research data, and they must be listed on an approved IRB protocol with a current human subjects training certificate.

- □ Conduct periodic access reviews and ensure individuals who no longer need access to the data are promptly removed.

- □ Do not email Protected Health Information (PHI) or Personally Identifiable Information (PII) without encryption. PHI should be shared using a Health Insurance Portability And Accountability Act (HIPAA) compliant method. Contact the TCIT Service Desk for information.

- □ Ensure you have a strong password and change it regularly. Passwords must contain at least 12 characters and include at least three of the following: lower-case, upper-case, numerical, or special characters.

- □ Transmit data over a public or private network in safe and secure ways, such as a Virtual Private Network (VPN). The networks at many data collection sites are public, and a VPN can help prevent data breaches. Contact the TCIT Service Desk to set up VPN access.

- □ Regulate physical access to fixed and removable data-storage media and devices (e.g., hard drives, laptops, paper files, etc.). Data stored in a location with physical access should be protected by swipe cards or keys controlled by the PI.

RESEARCH DATA STORAGE

- ☐ Research data, particularly identifiable data, should only be stored in TC-issued Google Drive accounts. Do not use personal accounts for storing data.

- ☐ If working with PHI, TCIT can provide a HIPAA-compliant Google account, which includes more secure (and more restrictive) versions of Gmail, Drive, Meet, and Calendar. Contact the TCIT Service Desk to request a HIPAA-compliant Google account.

SECURE DATA COLLECTION

For secure data collection use these tools:

- ☐ Qualtrics – A web-based survey tool for creating and conducting online surveys.

- ☐ REDCap – A secure web application for building and managing online surveys and databases.

If any other software or application is used for research purposes, it must first undergo a data security review. Contact the TCIT Service Desk to request a data security review.

- ☐ Do NOT use Survey Monkey or other free web-based data collection systems without first contacting TCIT. Many web-based systems are not secure and should only be used when collecting non-sensitive data.

SECURING PERSONAL DEVICES

Desktops and laptops can contain many vulnerabilities. To combat these vulnerabilities, TCIT recommends the following when using personal devices:

- ☐ Install the latest Windows (for PC) or Mac OS (for Mac) updates and a reputable malware software.

- ☐ Encrypt your computer and check your encryption status.

- ☐ Avoid storing research data on personal devices of any kind.

- ☐ Have a strong password. TCIT highly recommends and provides LastPass password manager to create strong passwords and securely store and share account credentials. Set a password-protected screensaver or screen lock that starts after 15 minutes of inactivity. This will reduce the length of time that an unmonitored machine is accessible to others.

DESTROYING RESEARCH DATA

All confidential data, regardless of storage location, will be retained only as long as mandated by the third-party agreements, research project duration, legal, regulatory, compliance, or business requirements. Contact TCIT Service Desk for guidance on the proper disposal of data.