Data Security Policy and Procedures

Berkeley Policy Associates Data Security Policy and Procedures follows:

BPA require all its employees and contractors to adhere to the company's data security policy and procedures. Separate guidelines are established for a different class of information. The overview of these guidelines are summarized below.

Definitions

Class 1: Confidential -- Anything that includes individual-identifying information such as names, SSN, dob. addresses, etc. These may include client and participant data as well as our personnel information.

Class 2: Business critical/Proprietary -- Any proprietary data and documents that are not Class 1. These may include program-level survey data, BPA's salary & sales info, and study notes and participant data without individual-identifying information.

Class 3: Not confidential.

Policies for Class 1 Data

(1) Can never leave BPA premises.
(2) Always kept in a secure place.
(3) Only authorized persons can access and use.
(4) Must be properly disposed of or transferred.

Procedures for Handling Class 1 Data

	Electronic Data	Paper Data
Receipt and tracking of Class 1 materials	▪ Notify office manager if expecting to receive confidential data ▪ Catalogue all data received	▪ Catalogue all data received ▪ Notify Office Manager if expecting to receive confidential data
Can never leave BPA premises	▪ Must work on BPA premises with these data (working from home/during business trip is not permitted)	▪ Must work on site with these data
Create separate working analysis file	▪ Strip individual-identifying information for analysis files, which can then be stored in access-limited folders on BPA's LAN	
Always kept in a secure place	▪ On data server or in locked cabinet in locked server room (CD or other disk media)	▪ Locked cabinet in a locked room ▪ Must not be left in public view (on desk or in common-use

	Electronic Data	Paper Data
	▪ Must not be left unattended in public view (e.g. on desk or screen) ▪ May not be stored on laptop	areas)
Only authorized persons can access and use	▪ Limit access to the data server by use of passwords ▪ The minimum number of people who absolutely need to use the data should be given access	▪ Key to locked cabinet to be kept securely by authorized persons ▪ The minimum number of people who absolutely need to use the data should be given access
Must be properly disposed of or transferred	▪ Update catalogue whenever data are disposed of or transferred ▪ Mail data in a password protected and/or encrypted form on an unmarked diskette and CD ▪ Require recipient and delivery verification. ▪ If absolutely necessary to transfer via email or internet, create encrypted, password-protected files; transmit password verbally (by phone). Do not include password in email!	▪ Update catalogue whenever data are disposed of or transferred ▪ When mailing, require recipient and delivery verification. ▪ Shred any paper with confidential data before disposing

Policies for Class 2:

(1) Only authorized persons can access and use.
(2) Must be used and stored under responsible person's oversight. Must not be left in public view (e.g. sitting out on a desk, open on computer monitor).