

## Data Security Exhibit

### 1. Protection of Data

The Researcher agrees to store the data received under this agreement on one or more of the following media and protect the data as described:

#### A. Hard disk drives

Data stored on local workstation hard disks. The data must be encrypted as described under G. data storage on portable devices or media. Access to the data will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

#### B. Network server disks

Data stored on hard disks mounted on network servers and made available through shared folders. Access to the data will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted on such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

When the data is stored on these disks, deleting unneeded data is sufficient as long as the disks remain in a secured area and otherwise meet the requirements listed in the above paragraph. Destruction of the data as outlined in Section 3. Data Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the secured area, at which time the data will be destroyed as outlined in Section 3.

#### C. Optical discs (CDs or DVDs) in local workstation optical disc drives

Data provided under this agreement, on optical discs, which will be used in local workstation optical disc drives and which will not be transported out of a secure area.

The data must be encrypted as described under G. data storage on portable devices or media. When not in use for the contracted purpose, such discs must be locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access the data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

#### **D. Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers**

Data provided under this agreement, on optical discs, which will be attached to network servers and which will not be transported out of a secure area. The data must be encrypted as described under G. data storage on portable devices or media. Access to data on these discs will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

#### **E. Paper documents**

Any paper records must be protected by storing the records in a secure area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

#### **F. Data accessed over the SGN or Internet**

When data is being transferred between Researcher and agency: Access to the data will be controlled by the agency providing the data, who will issue authentication credentials (e.g. a unique user ID and complex password) to authorized Researcher staff. Researcher will notify the agency providing the data immediately whenever an authorized person in possession of such credentials is terminated or otherwise leaves the employ of the Researcher, and whenever a user's duties change such that the user no longer requires access to perform work for this agreement.

The data shall not be transferred or accessed over the Internet between Researcher staff or Researcher-owned devices unless specifically authorized within the terms of the Agreement. If so authorized, the authentication credentials must provide a high level of confidence in the identity of the individual and the data must be encrypted during transmission, via a mechanism such as VPN or Secure FTP.

#### **G. Data storage on portable devices or media**

Portable devices include, but are not limited to; smart phones, tablets, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook/netbook computers

Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape), or flash media (e.g. CompactFlash, SD, MMC).

The data shall not be stored by the Researcher on portable devices or media unless specifically authorized within the terms of the Agreement. If so authorized, the data shall be given the following protections:

- Encrypt the data with a key length of at least 128 bits
- Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics.
- Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 10 minutes.

Physically protect the portable device(s) and/or media by

- Keeping them in locked storage when not in use
- Using check-in/check-out procedures when they are shared, and
- Taking frequent inventories

When being transported outside of a secure area, portable devices and media with data provided under this agreement must be under the physical control of Researcher staff with authorization to access the data.

## **H. Backup Media**

Data written to a medium and stored for backup purposes. Data may be backed up as part of Researcher's normal backup process provided that process includes secure storage and transport.

## **2. Data Segregation**

Data provided under this agreement must be segregated or otherwise distinguishable from all other data. This is to ensure that when no longer needed by the Researcher, all of the data can be identified for return or destruction. It also aids in determining whether the data has or may have been compromised in the event of a security breach.

The data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no other data. Or,

The data will be stored in a logical container on electronic media, such as a partition or folder dedicated to the data provided under this agreement. Or,

The data will be stored in a database which will contain no other data. Or,

The data will be stored within a database and will be distinguishable from other data by the value of a specific field or fields within database records. Or,

When stored as physical paper documents, the data will be physically segregated from all other data in a drawer, folder, or other container.

When it is not feasible or practical to segregate the data received under this agreement from other data, then all data with which it is commingled must be protected as described in this exhibit.

### 3. Data Disposition

When the research has been completed or when no longer needed, whichever is earlier, data shall be returned to the agency providing the data, de-identified per standards in the Privacy Rule (45 CFR 164.514(b)(2)), or destroyed using one or more of the following methods of destruction:

#### Data stored on:

#### Will be destroyed by:

Server or workstation hard disks

Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data

Degaussing sufficiently to ensure that the data cannot be reconstructed, or

Physically destroying the disk

Paper documents with sensitive or confidential data

Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of data will be protected.

Paper documents containing confidential information requiring special handling (e.g. protected health information)

On-site shredding, pulping, or incineration

Optical discs (e.g. CDs or DVDs)

Incineration or shredding

Magnetic tape

Degaussing, incinerating or crosscut shredding

Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)

Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data

Degaussing magnetic media sufficiently to ensure that the data cannot be reconstructed, or

Physically destroying the disk

#### **4. Notification of Compromise or Potential Compromise**

The compromise or potential compromise of the data must be reported to the contact indicated in this agreement within one (1) business day of discovery.