Data Security Plan

The Transfer Project

You may use this template to indicate the required security protocols that you will implement prior to receiving data from *The Transfer Project*, or you may use a template from your own institution that includes, at a minimum, the following security protocols:

1. Access to study data must be protected by a username and password that meets the complexity and change management requirements as follows:
    1. It must be at least 8 characters long (longer is stronger!)
    2. It must contain at least one letter
    3. It must contain at least one digit
    4. It must contain at least one of these characters: !@#$%&*+={}?<>"'
    5. It and your user ID must share fewer than 6 (or length of your user ID) consecutive common characters
    6. 8-15 characters: change password every 90 days
    7. 16 or more characters: change password annually
    8. *See additional notes on passwords below*

    _____ I agree to this security protocol
    user initials

2. Study data that are accessible over a network connection must be accessed from within a secure network (i.e., from on campus or via a VPN connection).

    _____ I agree to this security protocol
    user initials

3. Computers storing or accessing study data must have AntiVirus/AntiSpyware software installed and updated regularly where technologically feasible.

    _____ I agree to this security protocol
    user initials

4. Patch management and system administration best practices should be followed at all times on systems storing or accessing this study data.

    _____ I agree to this security protocol
    user initials

5. Users should be granted the lowest necessary level of access to data when technologically feasible.

    _____ I agree to this security protocol
    user initials

Additional notes for establishing and using strong passwords:

Because your password is your first line of defense against attack, it is imperative that you choose a strong password that cannot be easily cracked. This is especially important for administrator-level accounts. The System Administration, Network, and Security Institute (SANS.org) recommends certain guidelines for choosing an effective password.

- Many computers set an eight-character minimum for your password length. Even if yours does not, it is good to meet this recommendation. The longer your password, the more secure it will be.
- Always use a combination of upper- and lower-case letters and include special characters such as '~!@#$%^&*()-_=+{[]}\|`";:,/?.
- Do not base your password on any items of personal information (e.g. PID, Social Security number, street address, birthdays, names of family members, etc.).
- Do not attempt substitutions of numbers or characters that look like the letter they replace (e.g. C@R0L!N@ for CAROLINA); sophisticated password-cracking programs try these combinations as well.
- For stronger passwords, avoid words or combinations of words that could be found in an English dictionary, such as "ChapelHill".
- For best passwords, experts recommend acronyms for unusual phrases that you invent. An example would be the password "~2myuT$!" for "About 2 more years until Tenure $alary!"
- Change your password often, and do not write it down anywhere close to your computer.
- Do not share passwords with anyone. All passwords should be treated as sensitive, confidential information.

Here are some **don'ts**:

- Don't reveal a password over the phone to ANYONE, including computer support personnel. Support personnel should never initiate a call requesting a password.
- Don't reveal a password in an email message.
- Don't reveal or talk about a password to anyone, including co-workers or family members.
- Don't hint at the format of a password (e.g. "my favorite pet.")
- Don't reveal a password on questionnaires or security forms.
- Don't use the "Remember Password" feature of applications (e.g. Mozilla Firefox, Mozilla Thunderbird, Internet Explorer, or Outlook).