Brooks College of Interdisciplinary Studies

Policy on Securing Research Data

Introduction

Federal guidelines and laws (FERPA, HIPPA) are in place to prevent the sharing of personal information between parties without the consent of the individual. While conducting research, investigators may be obtaining personal and confidential information by consent of the research subject. However they are required to provide for the safe keeping of these data to ensure that it is not shared with parties outside the consent given by the subject. Therefore, best practice must be followed when securing data.

When collecting human data, consider first:

Is the personal information needed in order to conduct the research?

Are all descriptive data collected necessary for the effective execution of the study, or are some data being collected "just in case"?

When storing human data:

If stored on hard copy you must have a secure, locked location where the data can be stored. Access must be limited to only the investigators.

If stored on a computer, encrypted password access should be limited to investigators. Data backup is suggested, but this must also be stored in a password protected location. Be sure that the unit is aware of how you plan to store data.

If data collection is conducted via web-based, or on-line formats and stored on a server personal identifying information and IP addresses should be kept separate from the data, and data should be stored in encrypted format

When transporting data:

If data are being moved from one location to another, or processed using multiple computers-

- Do not transmit personal subject data via e-mail or other non encrypted method which could provide unauthorized users access to the information.
- Store on encrypted flash drives or writable media that secures the information from un authorized use.
- If hard copy data, transport in a secure container that prevents un authorized access.

Destroying data

Most researchers maintain research records for 5-10 years. If you are wanting to destroy data records be sure to follow the following practices:

Hard copy data- shred files using a shredder that will render the personal information un accessible

Computer data- Magnetic media (hard drives, tapes, CDROMs) which will have no further use should be physically destroyed (by crushing, drilling, shredding, or incinerating). Drives that will be reused should be sanitized using an appropriate program. Please utilize the IT department for the most up to date methods for sanitizing. Write-once media should be physically destroyed.

Security Suggestions

- **Be sure that someone can access your computer and files if you can't** for any reason. (Ask your computer systems support person to identify an appropriate mechanism.)
- **Update software regularly,** including anti-virus and security patches.
- **Don't waste bandwidth** by unnecessarily running file-sharing programs, Internet radio, streaming video, and other processes that use large amounts of memory.
- **Educate your co-workers** if they fail to follow good security practices, and notify your supervisor of any potential problems.