Data Security Standards
As of 02/2009

As a general practice research data (information collected/generated about individuals) should be stored separately from direct identifiers e.g. name, address, DOB, MRN, SSN) that can link the data to a person's identity. Instead, research data files should be stored using a unique "code" instead. The "linking code file" (code breaking list) should be maintained separately.

Securing the linking code file: The file that links the code to the person's identity (direct identifiers) should be maintained securely: if it is on paper it should be in a locked, secure place separate from the research data; if it is electronic, it should be encrypted, wherever it is stored.

Securing the research data file:
Research data files may currently be stored in various places, and their security requirements are different. Any research file stored on a desktop hard drive, stand alone server, laptop, flash drive, floppy disk, etc MUST be encrypted. If the research data file is kept on a personal network drive on the Academic Computing or Hospital IT file server located in the medical center's secure data center, encryption is not required, but still advisable. If the research data file is stored on a "departmental" network drive general drive for a whole department on the Academic Computing or Hospital IT file server located in the medical center's secure data center), access to the data files should be limited to the research team, either through restricted view access to team members set up by Academic Computing or Hospital IT (recommended) or password protection on the file. If this cannot be done, the files should be encrypted. Remember it is the location of the file, not the location of the computer that counts.

For questions on this topic, please contact the PPHS office for additional guidance.