GUIDANCE: Electronic Storage and Transmission of Study Data and Documents

Goal

To ensure study data and source documentation stored electronically meets the same fundamental elements of quality that are expected of paper records, and to make sure the electronically captured and shared data is secure, trustworthy and reliable.

ALL STUDIES: Use of Laptops, PDA, Jump Drives and other portable devices for Research

Regardless of type or sponsor of a research study, all research staff that utilize a laptop and/or other portable electronic device for data collection, analysis storage or transmission must take additional steps to ensure the data protection.

1. All laptops that access Boston Children's systems and data, including research, must be encrypted. If you are using a PDA, jump drive or other portable electronic device to store research-related information, we strongly recommend installing encryption software on these devices as well. For more information: http://ehelp.tch.harvard.edu/Encryption.html, "Frequently Asked Questions" or contact the ISD HelpDesk at help.desk@tch.harvard.edu or x5HELP.
2. As of May 8, 2012, mobile devices that access the Hospital Exchange system for email, calendar or contacts are required to create a secure PIN or password, via a security policy automatically sent to each device. The device locks after 15 minutes of inactivity, requiring the PIN or password to be re-entered. This includes all iPads, iPhones, Android devices and Blackberries. For more information: "Passwords on Mobile Devices Frequently Asked Questions"
3. If a laptop, mobile device, or any other portable data storage device containing any study data is stolen or lost, it must be reported to the CCI/IRB as an unanticipated event, and Information Security. Fill out a Lost or Stolen Device Form and contact both Physical Security (x56121 or 617-355-6121) and the Help Desk (5-HELP or 617-355-4357) as soon as possible.
4. In general, only store/work with research data on portable devices and laptops when necessary. And when necessary, implement a process to ensure all research data is backed up regularly, and removed as soon as possible.
5. Use best data security practices and follow CHB policy by using secure mail and secure file transfer procedures when exchanging Protected Health Information electronically with individuals external to BCH: See http://web2.tch.harvard.edu/ehelp/Documents/securemail.pdf and http://web2.tch.harvard.edu/ehelp/Documents/chbft.pdf

ALL STUDIES: Use a secure network system for research document storage

BCH supports a number of systems that facilitate collection and storage of research data on secure networks. These include the following:

- Children's Share (SharePoint) team sites - http://chbshare.chboston.org/TS/default.aspx and http://chbshare.chboston.org/elibrary/isd/educate/mer/Pages/spus.aspx . These sites support user-defined security, content versioning, and information presentation
- REDCap – a free, web-based, and user-friendly electronic data capture (EDC) tool for research studies. Useful for collecting and tracing information and data from research studies, scheduling study events, and conducting surveys. http://catalyst.harvard.edu/services/redcap/
- The Clinical Research Center published a guide to choosing the appropriate system: Clinical Research Databases and Web Survey Technologies.

Ensure that whatever system used has version control, adequate data security, training for users, and accessibility (PC and Mac users, on site and off site access for authorized users).

When storing study data electronically, please consider the following:

- Store all electronic data in a secure location that is password protected or requires user authentication. To setup a secure shared drive, please contact the HelpDesk at help.desk@tch.harvard.edu or x5HELP with the name of the share and who should have access.
- Retain all versions of study documents (all out-of-date versions and the current version).
- Ensure documents are stored so study staff can track all changes to ensure an audit trail. Documents still must be stored in a manner that procedures and results can be reproduced.
- Save versions at different pertinent time points: after a pre-determined number of subjects entered; after large data entry occurs; or substantial changes made to document.
- Routinely check documents to ensure data integrity: completeness, data points within appropriate ranges, etc.
- Establish, review and document security procedures to ensure only authorized individuals are permitted access to the data. If a study coordinator leaves CHB or your study group, remove their ability to access the data.
- Maintain and archive system documentation, SOPs and related artifacts (e.g., test results, staff lists).
- Ensure that system changes are documented thoroughly and software revisions are archived and applied correctly so that the data can be accessed in the future.
- Ensure safe and secure archival and accurate retrieval of electronic records.
- Train and evaluate all users to be sure they use the system properly.

Questions/Contacts

If you have any questions or would like more information, please contact us.

For study organization and documentation,	EQuIP (Eunice Yim Newbert or Susie Corl)
For laptop encryption software,	Information Security (isdsecurity-dl)
For Information Security questions,	Information Security (isdsecurity-dl) or visit http://web2.tch.harvard.edu/ehelp/mainpageS2853P39.html