

Security Guidelines for Clinical Research at Sparrow Health System

Introduction

This document was created to give you guidelines to follow in order to ensure that all confidential health information is protected as you procure, use, transfer, and store the data to complete your project. If you have additional questions after reading this document, a reference list is provided at the end to help you find answers to your questions.

Guidelines for Data Procurement

1. Follow all Institutional Research Review Committee (IRRC) policies and procedures when requesting data, including correctly completing all required forms and limiting your data requests to the minimum necessary for the purposes of the project.
2. De-identify data using one of the two approved methods: the statistical method or the “safe harbor” method. See HIPAA Policy, HP-22, De-identified Information for more information.
3. Follow the correct path to data procurement—direct all inquiries for data to Sparrow’s Information Services Decision Support team. Do not ask the Department manager or an IS Analyst. (Note: Chart review is excluded from this requirement.)

Guidelines for Data Use

Whenever possible, research should be conducted on a Sparrow asset (computer or other device). However, we also recognize that some of this work will necessarily be completed offsite or at other facilities.

1. If you need to work with electronic data on a non-Sparrow device (computer, laptop, PDA), the data should remain stored on a portable storage device (such as a portable USB drive) provided by Sparrow rather than being copied to the non-Sparrow device. As an example, if you have an electronic database stored on a USB drive, then you should actually open the database from that drive, rather than “copying” the database to your home computer and working on the data from that location. This reduces the risk of residual copies of data being left in unprotected areas (like a home computer).

Guidelines for Electronic Data Transfer

Electronic research data should only be transferred off of Sparrow property in one of the following ways:

- A) On Sparrow-owned portable media (USB drive or write-once media like a CD)
- B) Via a secure file transfer method (FTP with encryption for instance)
- C) Via email with appropriate encryption. In **no** case should data ever be transferred electronically (over the Internet) without appropriate encryption.

Paper copies of data, while not specifically addressed by these guidelines, should be handled with safeguards appropriate to any confidential PHI.

Guidelines for Electronic Data Storage

1. If you have access to a confidential directory on a Sparrow file server, store all research data in an encrypted format in that directory. If not, store all electronic data in an encrypted format on portable media provided by Sparrow (USB drive or write-once media like a CD).
2. Electronic data should not be stored on any non-Sparrow asset (including personal computers, laptops, PDAs, and other devices).

Guidelines for Project Completion (Data Destruction)

1. Investigator records must be retained, according to federal law (the “Common Rule” 45 CFR 46.115.7.b, and 21 CFR 312.62) for a specified period after the date that the study was completed. De-identified investigator records should be destroyed without being re-identified according to the following guidelines.
 - A) Electronic media should be returned to Sparrow’s IS Help Desk for proper decommissioning.
 - B) Once all retention requirements have been met, electronic copies of data on computers should be deleted off of systems (either Sparrow-owned or other devices) using a secure deletion utility. Contact the Sparrow Help Desk at 364-4357 for more information.

Thank you for taking the time to read this important communication, and for doing your part to ensure the privacy and security of Sparrow Health System’s Protected Health Information. If you have any questions about this process, please contact:

Sparrow Health System’s IRRC Coordinator
Suzanne Leialoha
364-2150
Suzanne.Leialoha@sparrow.org

Reference: *HIPAA Policy, HP-22, De-identified Information*
HIPAA Policy, HP-53, Use and Disclosure of Protected Health Information for Purposes of Research.
“Common Rule” 45 CFR 46.115.7.b

Approved: Institutional Research Review Committee: May 9, 2005