



Do's and Don'ts for e-Lab Notebooks

Boston
Delaware
New York
San Diego
Silicon Valley
Twin Cities
Washington, DC

Laboratory notebooks provide important legal information as well as scientific or engineering data. For example, lab notebooks may contain evidence related to priority of patent claims, as well as verification of compliance with regulations such as FDA guidelines for good laboratory practices (GLPs) and good manufacturing procedures (GMPs). Due to problems with authentication of the information contained in electronic versions of lab notebooks, electronic lab notebooks are not clearly acceptable in legal proceedings as a substitute for original, permanently-bound handwritten records, particularly with respect to proving dates of invention in patent cases. Until electronic records are fully approved and used by the courts, hard copy of all data should be maintained concurrently. However, following are guidelines to consider if you generate electronic data or maintain electronic records such as laboratory notebooks.

#1 — Do adopt an official procedure for electronic record-keeping

Establish a written policy that is furnished to each employee and adopt the policy as part of your normal business routine. Impart individual accountability in connection with the policy provisions.

#2 — Do generate permanent records

All electronic data should be backed up and write-protected, then clearly labeled, preferably to a “write once” media. If the original data is computer-generated, if feasible it should be printed in hard copy, labeled, signed, dated, and witnessed. All electronic data should be referenced in the handwritten notebook. Any hard copies should be attached permanently to the handwritten notebook, while electronic data should be stored in a safe place free from magnetic fields or other corruptive conditions. Both the hard and soft copies should be retained by record custodians who can vouch for their integrity, and all records/data should be maintained for the duration of the appropriate document retention period.

#3 — Do create accurate records

Electronic/digital signature or encryption hardware and/or software may be employed in order to enhance credibility of the electronic records. Precautions should be taken against the importation of viruses. Computer systems should be regularly validated to ensure reliability, accuracy, and consistent performance.

#4 — Do construct records that specifically reflect the evolution of the research

Hardware and/or software should be developed or used which prevents the ability of editing original research descriptions, i.e., WORM - Write Once, Read Many times. Additionally, all electronic records should be time-stamped by a separate server having highly restricted access.

#5 — Do protect records from unauthorized access

Security tools that prevent unauthorized access to the system should be implemented. Key and screen locks are useful, as well as removable storage devices that can be locked away when not in use. Access to the system should be limited to authorized personnel having a genuine need for such access. Distribution and use of information accessed from the system should also be appropriately limited. Log-on procedures should involve individual user codes and passwords that are changed frequently, and that are promptly removed from the system upon departure of an employee. Periodically, the network administrator should investigate to see who has accessed the system. ■

By **Diane L. Gardner**

FISH & RICHARDSON P.C.
Intellectual property and technology law
800 818-5070
www.fr.com
info@fr.com