

21 CFR Part 11 Checklist

FDA Compliance Tool

This tool is designed to help clinical researchers ensure that studies using computer systems to gather data electronically are in compliance with federal regulations. The checklist applies to any study that uses a computer system to enter data, whether the data is entered from a hardcopy, directly into the system, or automatically through a device (e.g., an ECG reading).

This document was compiled using the recommendations found in *Guidance for Industry: Computerized Systems Used in Clinical Investigations*, by the Food and Drug Administration, May 2007.

Phoenix Software International's Entrypoint helps clients conduct compliant clinical research studies using electronic data capture without the high cost and long implementation periods usually associated with EDC systems. With proper implementation and administration, clinical investigators can achieve full compliance as inventoried in this document using features available in Entrypoint Plus. Visit www.entrypointplus.com to learn more.

Study Protocols

1. Identify each step at which computer system will be used in written study protocol.
2. Submit protocol with Investigational New Drug (IND) and Investigational Device Exemption (IDE) applications.

Standard Operating Procedures

1. Have specific written operating procedures in place.
2. Make document available to personnel on site either in hardcopy or electronically.
3. Make document available for inspection by FDA.

Source document retention

(for data entered directly into computer system)

1. Treat electronic record as source document and retain as required under part 312, § 511.1(b).
2. When data is transmitted from one system to another or entered directly into a remote central computer system, maintain copy in another location as defined below (check one).
 - a. At clinical site.
 - b. Another location (e.g., a data storage facility).
3. Produce copies contemporaneously with data entry.
4. Preserve copies in appropriate format such as XML, PDF or hardcopy.

Internal Security

1. Access Limitations
 - a. Password-protect individual accounts.
 - b. Configure computer system to require manual login and logout.
 - c. Automatically limit number of failed login attempts.
 - d. Automatically record unauthorized login attempts.

- e. Do not share individual account access with other users.
 - f. Do not log on to system to provide access to another user.
 - g. Electronically require users to change their passwords at regular intervals.
 - h. Automatically password protect computer systems when idle for short periods.
 - i. Automatically log users off computer systems when idle for long periods.
2. Audit Trail
 - a. Keep track of all creations, modifications, and deletions electronically.
 - b. Maintain all entered data: Don't obscure original data when changes are made.
 - c. Time stamp change automatically.
 - d. Configure computer system to require user to record reason for change.
 - e. Automatically record identity of individual who made change.
 - f. Prevent users from being able to modify or delete audit trail.
 3. Date and Time Controls
 - a. Synchronize computer system to date and time provided by international standards setting source (e.g., <http://www.time.gov/>)
 - b. Limit user's ability to change time.
 - c. Document all date and time changes (except daylight savings time).
 - d. Include year, month, day, hour, and minute in time stamp
 - e. Include time zone in date and time stamp.
 - f. Explain any time zone references and naming conventions in study documentation.



External Security

1. Restrict access to computer system and data via external software applications by encrypting data as it is transferred and/or using a firewall.
2. Maintain cumulative record that indicates names of authorized personnel, their titles, and a description of their access privileges.
3. Prevent, detect and mitigate effects of viruses and other harmful software code.

Other Features

1. Direct Entry of Data
 - a. Use prompts, flags, and other help features to encourage consistent use of terminology.
 - b. Use prompts for data out of the specified range. Specify valid vs. invalid ranges and alert user.
 - c. Do not set up system to enter default data if field is bypassed.
 - d. You may allow system to populate field with data duplicated from another field. However, analyze potential consequences very carefully before doing so.
2. Retrieving Data
 - a. Design computer system to attribute data record to each individual subject.
 - b. Be able to reconstruct source documentation for FDA review.
 - c. Be prepared to fully describe to FDA how data were obtained and managed.
3. Document what software and hardware is used.
4. System Controls
 - a. Set up a full backup and recovery system to protect against data loss if records are maintained only in electronic form.
 - b. Ensure that backup system maintains data integrity.
 - c. Store backup records at a secure offsite facility.
 - d. Maintain backup and recovery logs.
5. Change controls
 - a. Maintain data integrity when making changes to the computer system, such as software upgrades, security and performance patches, equipment repairs, etc.
 - b. Carefully evaluate effects of any changes before and after making them.
 - c. Validate changes that exceed previous operational limits.
 - d. Document all computer system changes.

6. Training
 - a. Ensure that individuals who develop, maintain and use computer system have sufficient education, training, and experience to perform tasks
 - b. Document computer education, training, and experience of personnel.
 - c. Provide training in the operation of the computer system led by qualified individuals as needed.
 - d. Conduct training sessions as needed on a continuing basis in case of changes in personnel and the computer system.

About Phoenix Software International

Phoenix Software International, Inc. is a major systems software development company providing advanced software solutions to enterprises around the world. Our diverse products support IBM and compatible mainframes, personal computers, and local and wide-area networks. Phoenix customers range from small entrepreneurial companies to major federal and state agencies to Fortune 500 leaders.

Phoenix develops Entrypoint Plus software expressly designed for creating, deploying, and administering custom clinical trial applications. The software was introduced in 1981 and was one of the first products available for electronic data capture. Entrypoint Plus is the software of choice for organizations that have been using EDC since the technology began.

Today, Entrypoint Plus uses a scalable, client-server network architecture with an ODBC interface to relational databases. Entrypoint Plus has special features for clinical trials including electronic CRF templates, powerful security options, a full audit trail, comprehensive field checking, remote data entry, and more.