OnlineCRF

SMART & EFFICIENT

Computerized Systems used in Clinical Investigations Requirements

Compliance checklist

OnlineCRF is compliant with the following requirements:

Study Protocols

- ✓ Computerized systems should be designed in the following way:
  - to perform the processes assigned to these systems for use in the specific study protocol;
  - to prevent errors in data creation, modification, maintenance, archiving, retrieval, or transmission.

Standard Operating Procedures

- ✓ There should be specific procedures and controls in place when using computerized systems to create, modify, maintain, or transmit electronic records, including the collection of source data at clinical trial sites.
- ✓ SOPs should be maintained either on-site or be remotely accessible through electronic files as part of the specific study records and the SOPs should be available to use by personnel and for inspection by the FDA.

Source Documentation and Retention

- ✓ When source data are entered directly into a remote computerized system or an electrocardiogram at the clinical site is transmitted to the sponsor's computerized system, a copy of the data should be maintained at another data storage.

Internal Security Safeguards. Limited Access

- ✓ Access must be limited to authorized users.
- ✓ Each user has an individual user account.

- ✓ The system should be designed to limit the number of log-in attempts and to record unauthorized access log-in attempts.

- ✓ The system should not allow a user to log in to provide another person access to the system.

- ✓ An automatic log out function should be appropriate for long idle periods.

Internal Security Safeguards. Audit Trails

- ✓ Computer-generated, time-stamped audit trails or other security measures capture information related to the creation, modification, or deletion of electronic records.

- ✓ Users who create, modify, or delete electronic records should not be able to modify the documents or security measures used to track electronic record changes

- ✓ Audit trails or other security methods used to capture electronic record activities should describe when, by whom, and the reason changes were made to the electronic record.

- ✓ Original information should not be obscured through the use of audit trails or other security measures used to capture electronic record activities.

Internal Security Safeguards. Date/Time Stamps

- ✓ Controls should be established to ensure that the system's date and time are correct.

- ✓ The possibility to change the date or time should be limited to authorized users. And such users should be notified if a system date or time discrepancy is detected.

- ✓ Any changes to the date or time should always be documented.

- ✓ Date and time are local to the documented activities and include a year, month, day, hour and minute.

External Security Safeguards

- ✓ External safeguards should be put in place to ensure that access to the computerized system and to the data is restricted for authorized users.

- ✓ Staff should be thoroughly kept aware of system security measures and the importance of limiting access for authorized users.

- ✓ Procedures and controls should be put in place to prevent the altering, browsing, querying, or reporting of data via external software applications that do not enter through the protective system software.

- ✓ A cumulative record should maintain the names of authorized users, their titles, and a description of their access privileges for any point in time.

- ✓ Controls are implemented to prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software.

Other System Features. Direct Data Entry

- ✓ Prompts, flags, or other help features should incorporate into a computerized system to encourage consistent use of clinical terminology and to alert the user of data that are out of acceptable range.

- ✓ The programming features that automatically fill out a field when the field is bypassed (default entries) should not be used.

- ✓ The programming features that permit repopulation of subject's specific information can be used.

Other System Features. Retrieving Data

- ✓ The computerized system should be designed in order to retrieve data regarding each individual subject in a study.

Other System Features. Dependability System Documentation

- ✓ For each study, documentation should identify what software and hardware will be used to create, modify, maintain, archive, retrieve, or transmit clinical data.

Other System Features. System Controls

- ✓ Records should regularly be backed up in a procedure that would prevent a catastrophic loss and ensure the quality and integrity of the data.

- ✓ Backup and recovery logs are maintained.

OnlineCRF

SMART & EFFICIENT

Training of Personnel

- ✓ Those who use computerized systems must determine that individuals who develop, maintain, or use computerized systems have the education, training, and experience necessary to perform their assigned tasks.
- ✓ Training should be provided to individuals in the specific operations with regard to computerized systems.
- ✓ Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerized system and with any changes to the system during the course of the study.
- ✓ Employee computer education, training, and experience are documented.

PHARMAXI

Poland, 50-148, Wroclaw, Wita-Stwosha 16

Phone: +487 171 660 44

www.pharmaxi.pl

www.onlinecrf.com

info@onlinecrf.com