

Sponsor Hosting of eSource Data

For the purposes of this comment the following definitions will be used:

eSource: Data captured directly onto an eCRF where no intermediary source exists

Hosting: Hosting means providing the computer facilities (servers) and procedures for a safe custody/storage of clinical data in such a way that data is protected against un-authorized access during and after a trial. The host is responsible for ensuring the ALCOA-principles are met at all times.

There has been strong and consistent lobbying of the FDA in support of the theory that eSource data is potentially open to systematic fraud in the hands of a sponsor and as such should be hosted by a Trusted Third Party company. However no substantial evidence appears to be available to support this position and the motives of the companies and individuals (or their sponsors) undertaking the lobbying is at best open to charges of conflict of interest.

The contention is that without viable hard copy documentation and with the possibility of low level database access that undocumented changes to data may be introduced in order to favourably modify the outcome of a study or series of studies. This contention is based on the assumption that Data Base Administrator (DBA) access to a database is below the level of control afforded by Clinical Data Management Software (CDMS) and therefore cannot be audited by these systems. This is correct but ignores the fact that all Data Base programs include internal auditing facilities that may be utilised to supplement and support the CDMS audit trail thus providing data audit information for any level of access.

The hosting of clinical trial data, with or without a hard copy source document should be viewed as a trusted process within the clinical trial process in the same manner as, for example, code randomisation or data blinding. The FDA has long accepted that these and other functions with potential for the introduction of fraud may be under the control of the sponsor providing that suitable procedures for control and confidentiality are demonstrably evident. Given that the same or a greater level of controls and procedures are evident for hosting of eSource then a similar level of trust should be applicable to this function.

To ensure the integrity of the eSource data there must be clear and defined separation of the database management and clinical data management tasks and the reporting structures of the groups or individuals involved in these tasks

The following must be regarded as the minimum level of security and separation:

- ~~✍~~ Clinical data shall be stored in a secured, validated database environment.
- ~~✍~~ Data storage will be in a manner such that access will be only permissible at a database level (i.e. outside of the control of the CTMS software) via the database account designated as the data owner.
 - Creation and maintenance of the data owner account shall be under the control of a data base administrator. The data base administrator shall be outside of the clinical study management group and shall have direct line reporting to a manager outside of this group.
- ~~✍~~ The database environment utilised shall provide an internal audit trail that shall be activated to log all access by the data owner account.
 - Application and control of this audit function shall be outside the control of the clinical study management group. The person or persons undertaking this control shall have direct line reporting to a manager outside of this group.
 - A certified, searchable, human readable, electronic version of this audit log shall be included in materials provided to the investigator on study closeout.
- ~~✍~~ Modify access to data for clinical purposes (data management, cleaning etc.) shall only be permissible via the CDMS software