**End of Study Data activities**

The below sequence broadly describes the process:

* Data received and all queries resolved (Prior to End of Trial (EoT) notification being submitted to Research Ethics Committee (REC) and Medicines & Healthcare products Regulatory Agency (MHRA))
* Final quality check to ensure all data present, correspondent and accurate
* Data Lock
* Data release

**1. Data received and all queries resolved (Prior to EoT notification being submitted to REC and MHRA)**

Appropriate checks at this stage may include:

* Check that all expected Case Report Forms (CRF) have been entered.
* Check that the project database is consistent with the specifications in the project data dictionary.
* Determine the status of each subject entered (i.e., excluded, ongoing, completed, withdrawn, lost to follow-up, etc.).
* Check for value formatting problems in database exports.
* Check for consistency between whole-date fields and associated part-date fields.
* Confirm that all expected site signatures have been applied.

**2. Final quality check to ensure all data present, correspondent and accurate**

Type and amount of quality checks should be determined by the nature of the study and the potential uses of the data.

Detailed quality assurance procedures to be performed to ensure all possible errors are detected and corrected before database lock. For example, an audit may be performed of a sample of completed CRFs in the Electronic Data Capture system against exported SAS datasets to ensure the integrity of the final study data.

If a separate soft lock will take place prior to final lock, describe how the two events will take place and what may distinguish soft from hard lock in terms of user access and write privileges.

All the data management activities must be concluded preceding the database lock.

These checks can include discrepancy management, batch validation, medical coding

A clear decision should be made and documented that the database is ready for analysis.

Only when this has occurred should the team progress to data lock.

**3. Data lock**

Data lock is performed to prevent further changes being made to the data and to clearly define which dataset was used to conduct analysis.

Data lock procedures should be fully documented in the Data Management Plan (DMP).

Data lock procedures should ensure that the data set used for analysis is clearly identified.

This should be retained separately from the live database to allow reproducible analyses.

It is a controlled procedure that freezes the data in a particular format securing the trial data and preventing further changes.

There is a requirement to ensure all the trial data have been received, verified, fully coded and cleaned for analysis with all queries resolved before locking the database for further analyses.

Unlocking of the database should be strictly controlled and documented in the DMP.

A pre-lock checklist should be prepared and successful completed prior to locking.

The DMP should clearly lay out the stakeholders who need to consent prior to data lock.

Post locking; the database cannot be altered in any way. However, only in case of a critical issue or any crucial operational reasons, Chief Investigator (CI) can authorise access and amend the data even after the database is locked. However, this needs to be robustly documented and an audit trail to maintained with satisfactory explanation for updating the previously locked database.

**4. Data release**

Following data lock, data can be released for analysis following the DMP. CI is responsible for ensuring and SAP is in place prior to data release