
Database Closure

October 2013

Abstract

Study databases must have access removed and be properly closed to ensure data integrity for the generation of results, analyses and submissions. This chapter recommends processes, checklists, and essential documentation for locking and closing study databases. Reopening a locked database to evaluate and correct errors is discussed, with an examination of important considerations and decisions that should be made, procedures that should be followed, and documentation that must be produced.

Introduction

At the culmination of a clinical study, database locking and closing procedures are imperative to prevent inadvertent or unauthorized data changes prior to analysis and reporting. For blinded studies, database closure procedures must also ensure blinding is not broken prematurely or by unauthorized personnel. Because data integrity and blinding are crucial to the success of a study, all clinical studies must have well-defined and documented processes for locking, unlocking, and closing study databases.

Terminology varies among different organizations, database systems, and clinical data management systems (CDMS), in particular regarding terms such as “interim lock,” “soft lock,” “final lock,” “database freeze,” and “database closure.” For the purposes of this chapter, the following definitions specify the meaning of some of the terms used in this chapter. These terms may be interpreted differently within different organizations.

- *Interim lock* refers to processes used to take a “snapshot” of a database at a particular point in time while the study is still in progress.

- *Soft lock* refers to processes during which access to the database is limited while CDM personnel confirm the suitability of the data for final analysis.
- *Final lock* (also known as a “freeze” or “hard lock”) refers to processes used to remove access to the database to ensure no further changes to data can be made. The final lock is a key process of database closure, but not the only process needed to close a database properly.
- *Database closure* refers to processes used to finalize the database as a final study deliverable.

These terms are not defined universally within the clinical research industry, so clinical data management (CDM) personnel should ensure they clearly understand how these terms are used or how they relate to terminologies used within their specific organizations.

Scope

This chapter describes distinctions between interim lock, soft lock, final lock, and database closure procedures, as well as discussing considerations for unlocking and relocking a database. The importance of a thorough database closure checklist is discussed, and a sample database closure checklist is provided.

Although some of the specific topics addressed by this chapter may not be the direct responsibility of CDM personnel, data managers must have an ongoing awareness of requirements and ensure these tasks have been completed in accordance with the principles and standards of their organization, regulatory bodies, and good clinical practice.

Minimum Standards

- Establish clearly documented procedures defining all steps of database lock, database closure, and unlocking and relocking the database after database closure.
- Clearly define all roles with respective responsibilities involved with database lock and closure procedures.

- Prior to database lock (interim, soft, or final) or database closure, ensure documentation of all defined tasks or criteria has been completed.
- At final database lock, ensure all team members are notified and access that allows database changes is removed and documented.

Best Practices

- Clearly define all terms relating to interim lock, soft lock, final lock, database unlock and final database closure.
- Develop and utilize a database closure checklist.
- Maintain documentation and approval or acknowledgement documents requiring signatures of all responsible parties involved in database lock, unlock and closure procedures.
- Where indicated, plan an interim or soft lock with a statistical analysis and data review prior to the final lock. This review may identify potential data errors, preventing the need to unlock the database after the final lock.

Interim and Final Lock Distinctions

Interim locks create a snapshot of a database at a particular point in time, and are typically performed to facilitate statistical analyses, listings, and reports prior to completion of the study. During the interim lock, access to the data to be analyzed may be restricted to certain personnel for a set period of time or until specific criteria are met. This restriction of access minimizes the possibility of inadvertent or unauthorized changes being made to the data. Because a study is often still in progress during an interim lock, the database will frequently have unresolved queries. Interim locks are often associated with some degree of data-cleaning activities, although data may not be cleaned as thoroughly as with a final lock. For example, data cleaning activities for an interim lock may be limited to critical data affecting safety and efficacy.

A final lock is only performed at the end of a study and is one of the initial steps toward complete study closeout. Once final lock has occurred, no changes to data can be made, and access to the database is typically restricted to only those personnel responsible for closing, delivering, and archiving the

database. Multiple interim locks may be performed in preparation for the final lock, allowing new or updated information that needs to be incorporated into the database prior to final lock. Before the final lock is initiated, all data queries are resolved, all medical coding is complete and approved, all external data reconciliation is completed and approved, and all data should be cleaned thoroughly. Some organizations may perform a soft lock prior to the final lock to ensure all activities required for the final lock have been adequately performed. Should it become necessary to unlock the database after the final lock has been initiated, database unlocking criteria and procedures typically become much more stringent than those for a soft lock or interim lock.

Minimum Requirements for Database Lock

Prior to database lock, the data manager should make certain the following tasks have been completed in accordance with established procedures and quality standards.

- For any database lock, identify and document the personnel responsible for performing various tasks for the database lock at the start of the project. Any subsequent changes in these roles or responsibilities must be documented. For more information on responsibility matrices see the GCDMP chapter entitled “Project Management for the Clinical Data Manager.”
- Notify relevant stakeholders and study team members in advance when an interim or final lock is to occur, then follow up with a notification when the lock occurs.
- For a final lock, ensure all applicable data have been received, processed and source verified (paper studies) or electronically signed by the principal investigator(s) (EDC studies). For interim locks, the degree of data processing and source verification may not be held to the same level as for a final lock.
- For a final lock, ensure all queries have been resolved. For interim locks, all queries may not need to be addressed, although all efforts should be made to resolve any critical queries potentially impacting interim analyses.

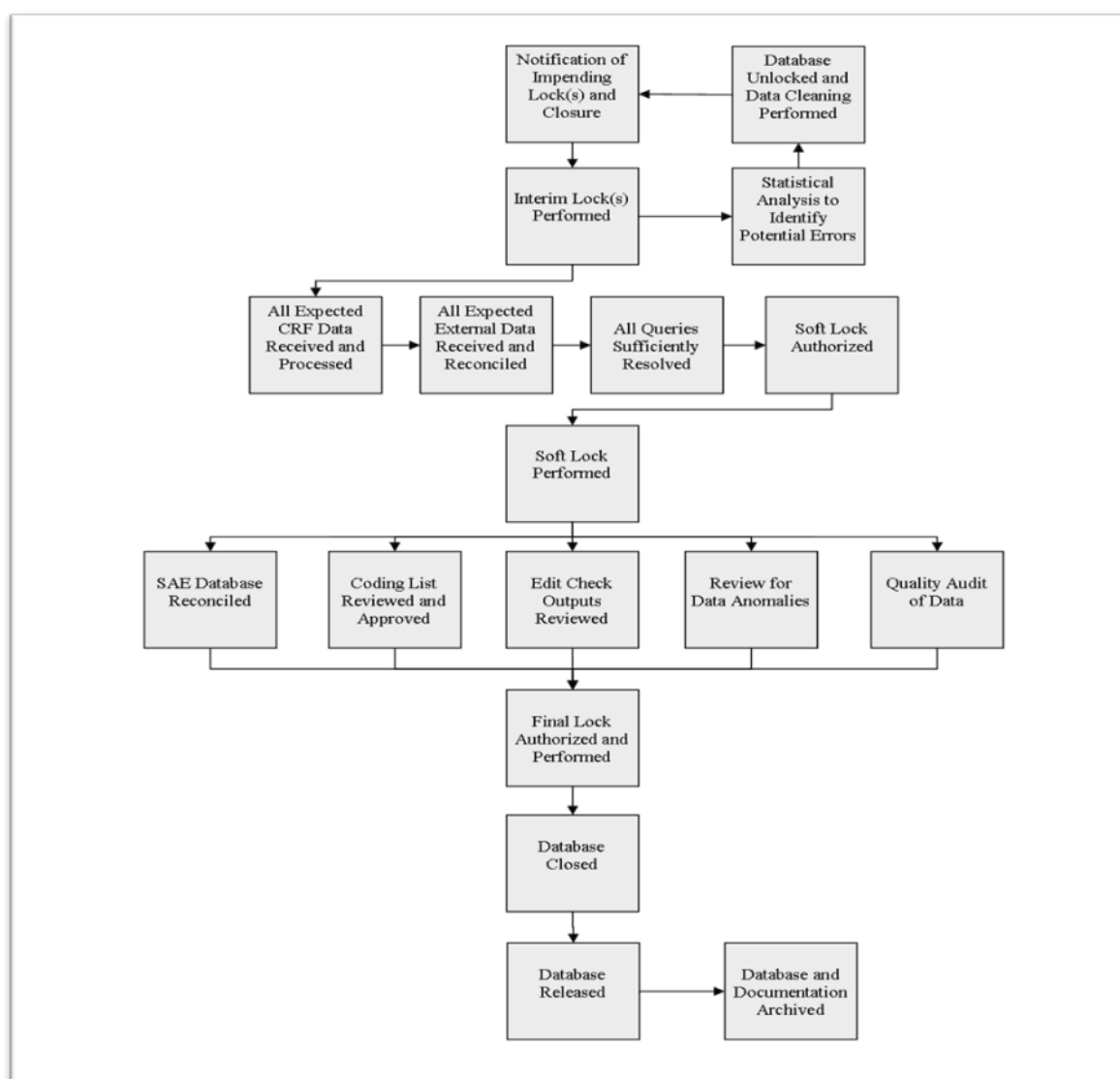
- For a final lock, ensure all expected external data (e.g., electronic laboratory data, IVRS, ePRO, ECG, etc.) are received, complete and reconciled with the study database. Interim locks may be performed with incomplete external data, but an effort should be made to reconcile external data that have been received.
- If a separate database exists for serious adverse events (SAEs), it should be reconciled with the main study database.
- The coding list (i.e., for adverse events, concomitant medications, etc.) should be reviewed for completeness and consistency, and should be approved by a medical monitor or safety surveillance team, if applicable.
- Ensure a final review of logic and consistency check output (edit checks) and data listings/patient profiles has been performed.
- Ensure a final review for obvious data anomalies has been performed.
- Perform a quality audit of the data and document the corresponding error rate. In many organizations, this audit may be performed by a separate quality assurance department. For more information on data quality, see the GCDMP chapter entitled “Assuring Data Quality.”
- Every database lock should follow a documented approval process with approval or acknowledgement by relevant study personnel (e.g., data manager, biostatisticians, monitoring representative, clinical/scientific representative). The ability to edit the database (“edit access”) should only be removed after the necessary approvals have been obtained, and the date of edit access removal should be documented.
- For any database lock, all documentation should be updated and stored according to standard operation procedures.

Database Closure Processes

Before a database can be closed, the final database lock must be completed and documented, including documentation that all edit access was removed at a defin-

itive point in time. Before the final lock is performed in preparation for database closure, clearly defined procedures must be followed to ensure all data have been received and processed, all data meet an acceptable quality level, and all relevant study personnel and stakeholders have been notified or have approved the final database lock. In addition to the tasks performed for a final database lock all documentation for database closure should be updated and stored according to standard operating procedures. Figure 1 shows a sample workflow of the main process steps of database closure.

Figure 1: Sample Database Closure Steps



Database Closure Checklist

Every study should have a database closure checklist that should be closely followed to ensure all required tasks have been performed. Each task on the checklist should indicate who is responsible for the task and be accompanied by the date of completion and the signature or initials of the individual responsible for confirming the task was satisfactorily completed. For a sample database closure checklist, see Figure 2.

Figure 2: Sample Database Closure Checklist

Task	Role Responsible	Date Completed	Signature
Study team and stakeholders notified of database lock/closure.			
All applicable CRFs/data received, entered, and source verified.			
All external data received and reconciled.			
All queries sufficiently resolved.			
Final database lock approved and performed.			
SAE database reconciled.			
Coding list reviewed and approved.			
Final review of edit check outputs performed.			
Final review of data listings and patient profiles performed.			
Final statistical review for data anomalies performed.			
Quality audit of data completed.			
Database release authorized.			
Database release completed.			
Database archived.			
All required database lock and closure documents present.			

Although some elements of a database closure checklist should be relatively universal, other elements may be specific to the organization, study, CDMS, or database. In creating the checklist, the following documents and personnel should be consulted to determine the applicable items to include on the checklist.

- The organization's standard operating procedures
- Software platform requirements of the CDMS or database
- Protocol requirements
- Data management plan requirements
- Input from clinical, biostatistics, programming, and quality assurance personnel

Database Lock and Closure Documentation

All database locks and closures should be clearly documented, including all of the steps that go into the lock or closure. This documentation should include the reasons for any interim locks, the signed database closure checklist, and documentation of all tasks that comprise the lock or closure (e.g., final data receipt, SAE database reconciliation documentation, etc.). For most individual tasks that are part of the database lock or closure, documentation should include the date of completion and the signature or initials of the study team member(s) responsible for the task. Some organizations may archive the results of data quality audits with database closure documentation, but other organizations document data quality results separately.

Final Database Release

After a database has been closed with appropriately signed authorizations and documentation, the database is ready for release. Details of database release vary widely between organizations, particularly between CROs and sponsors. For example, a CRO may release the database directly to the sponsor, whereas a sponsor might release the database to a separate department within the organization. Regardless of the entity to which the database is to be released, the release should only be performed with signed authorization or acknowledgement.

If a study is blinded, release of the database is typically necessary prior to unblinding of the data. Although the data must be unblinded prior to statistical analyses, unblinding the data too soon can pose risks to the overall success of the study. Because of the magnitude of risk posed by premature unblinding, documented authorization for final database release is arguably even more crucial for blinded studies. Documented authorization should also precede unblinding of the data. In some situations, data is unblinded within the CDMS prior to final database lock and release. However, in these situations documented authorization for unblinding is still a crucial step.

EDC and Paper-Based Distinctions

Although there are differences in database lock and closure procedures between EDC and paper-based studies, these distinctions are often specific to the EDC systems that are used. For EDC studies, CDM should ensure that Principal Investigator(s)' electronic signatures are compliant with 21 CFR Part 11, which details the FDA's requirements for electronic signatures.¹ Source document verification procedures are also quite different between EDC and paper-based studies. In EDC systems, access to the database may be restricted to "read only" at the lock stages followed by complete removal of access occurring after database closure. For more information about distinctions between EDC and paper-based studies, see the GCDMP chapters entitled "Electronic Data Capture—Concepts and Study Start-up," "Electronic Data Capture—Study Conduct," and "Electronic Data Capture—Study Closeout."

Database Unlocking/Relocking

Ideally, a final lock should be truly final, and subsequent unlocking is discouraged. However, certain circumstances may necessitate temporarily unlocking the database after final lock has occurred. Before a request to unlock a database is authorized, appropriate management at the organization should carefully review the reasons provided to justify unlocking the database.²

Whenever there is a need to unlock a previously locked database, documented authorization should be received before unlocking commences. A thorough evaluation should be made before deciding to unlock a database. Well-defined

policies and procedures should be followed to ensure unlocking restores access to authorized personnel only. Although discouraged, any data changes made while the database is locked must be captured within the audit trail.

Despite being discouraged, unlocking a database after final lock occurs frequently enough that organizations should have policies in place to manage the details of unlocking. These policies should clearly define the reasons for unlocking a database after final lock, procedures to be followed when unlocking or relocking, and procedures to be followed for the period between unlocking and relocking. Procedures should include notification of the study team, a clear definition of the change(s) being made, the date changes are implemented, the specific individuals who will regain access to the database, and steps to ensure that only the authorized changes and no others have been made. Relocking the database should follow the same or similar processes for notification and approval as the initial lock.

Note that not all errors found after final lock must be corrected in the database itself. Most large clinical databases are not completely free of errors. The database should only be unlocked due to data errors relating to safety or efficacy parameters that may impact the statistical analysis and conclusions drawn from the study. Some errors may be documented in the statistical or clinical report. Some organizations may maintain a database error log that lists each error, the action taken, the reason why the database was not unlocked to correct the error, and who made the decision to not unlock the database. Regardless of the specific strategy employed by an organization, organizations should implement predefined processes to determine how such errors will be handled and documented.

Recommended Standard Operating Procedures

- Interim Database Lock
- Final Database Lock
- Database Unlock/Relock
- Database Closure
- Change Control/Errors

References

17. *Code of Federal Regulation, Title 21, Volume 1, Part 11: Electronic Records, Electronic Signatures*. Washington, DC: Government Printing Office; 1998.
18. Prokscha S. *Practical Guide to Clinical Data Management*. New York, NY: CRC Press, 2007:75-88.

Further Reading

Terms used in this chapter may be found in the *Good Clinical Data Management Practices* Glossary.

Chapter Revision History

Publication Date	Comments
September 2000	Initial publication.
May 2007	Revised for style, grammar, and clarity. Substance of chapter content unchanged.
October 2013	Revised for content, style, grammar, and clarity with database closure sample flowchart and sample checklist added.

This page is intentionally blank.