# Teradata Solutions: Helping You on Your Journey to Part 11 Validation

LIFE SCIENCES INDUSTRY SOLUTIONS

Biopharmaceutical drug development and manufacturing operations demand robust applications to facilitate the discovery, development, and production of their drugs. These applications automate the often tedious tasks that regulatory agencies demand, enabling you to focus on what you do best. Nowhere is this need for automation more apparent than with the rigorous recordkeeping requirements of 21 CFR Part 11. These FDA regulations, designed to permit the widest possible use of electronic technology for maintaining electronic records, electronic signatures, and handwritten signatures executed to electronic records, describe in detail the types of controls required to leave behind the paper world.

Teradata can help your company meet its Part 11 obligations by offering a relational database management system that has been independently audited by a third party compliance organization, Compliance Implementation Services (CIS), and found to address all aspects of the regulation that a database product can meet. Its extensive logging capabilities, access controls, and compatibility with the most popular authentication methods gives you the flexibility to implement data collection and analysis applications with the confidence that the underlying database will not hinder compliance efforts.

## The Teradata Approach to Part 11 Compliance

CIS conducted rigorous testing of the Teradata® Database system controls and business requirements to ensure its compliance with 21 CFR Part 11 requirements. The audit activities included:

- **Compliance Documentation Review:** CIS reviewed existing documentation, including design specifications, process plans, Standard Operating Procedures (SOPs), and other supporting documentation to determine compliance with 21 CFR Part 11 requirements.
- **Business Process Review:** CIS performed interviews with key stakeholders and system walkthroughs in pertinent functional areas to identify the business requirements for the system and the workflows employed; aligning communicated information to system design and system specifications.
- **Data and Systems Review:** CIS evaluated system documentation, including system development, security overview, data extraction and validation reports.
- **IT Controls Testing:** CIS executed testing related to access security by performing walkthroughs within the system and testing key attributes as it pertains to 21 CFR Part 11. Key areas of testing included, but were not limited to, logical controls over infrastructure applications and data, the change controls process, user acceptance testing, training records, and backup and recovery procedures.
- **Audit Readiness:** CIS evaluated the system's capabilities and responsiveness to request for documentation and data.

We understand the opportunities for paperwork reduction that Part 11 offers you—and we understand the challenges it poses as well. That's why we've created a system that addresses every aspect of Part 11 that it is possible for a database product to address. With Teradata Database in place, your journey to Part 11 validation receives a significant boost.

## For More Information

To learn more about how Teradata can help you with Part 11 validation, contact your Teradata representative or visit Teradata.com.

## How Teradata Addresses Part 11 Requirements

System controls, documentation, processes and procedures were reviewed in place to assess the compliance with the following FDA requirements set forth below in 21 CFR Part 11:

| Part 11 Requirement | The Teradata Approach |
|---|---|
| 21 CFR § 11.10(a)<br>System validation | Teradata Database has successfully undergone an intensive scrutiny of all security controls by Compliance Implementation Services, a third party compliance company. |
| 21 CFR § 11.10(b)<br>Accurate and complete copies of records | Teradata Database ensures that all changes are documented and can hold individuals responsible for changes through extensive logging capabilities. |
| 21 CFR § 11.10(c)<br>Protection of records | Teradata Database can enforce strict rules with respect to retention. For example, permissions for select, create, modify, and delete can be assigned separately. |
| 21 CFR § 11.10(d)<br>Limiting system access | Teradata Database implements strict login security controls that ensure that only authorized individuals can gain access to the database, including password complexity restrictions and encrypted credential exchanges. |
| 21 CFR § 11.10(e)<br>Computer-generated audit trail | Teradata Database can log each and every database access including selects, writes, and deletes. |
| 21 CFR § 11.10(f)<br>Operational system checks | Teradata Database can enforce separation of duties and check to ensure that users are permitted to execute the appropriate SQL statements. |
| 21 CFR § 11.10(g)<br>Authority checks | Teradata Database implements strict login security controls that ensure that only authorized individuals can gain access to the database. |
| 21 CFR § 11.10(h)<br>Devices checks | The Teradata Director Program Identifier enables each Teradata client to be assigned a separate host identifier. This allows Teradata to restrict access not only by username and password, but also client workstation. |
| 21 CFR § 11.10(i)<br>Education and training of personnel | The Teradata Database system comes with an extensive library of documentation to assist administrators and end users. |
| 21 CFR § 11.10(j)<br>Personnel accountability | The Teradata Security Administration manual provides guidance for sound security practices related to the security of the overall operating environment. |

| Part 11 Requirement | The Teradata Approach |
|---|---|
| 21 CFR § 11.10(k)<br>Control of documentation | N/A |
| 21 CFR § 11.30<br>Controls for open systems | Teradata Database offers extensive encryption options for data in transit. By default, all logon strings are encrypted between the client and server, and when stored in Teradata Database, passwords are encrypted. |
| 21 CFR § 11.50<br>Signature Manifestations | Teradata Database can record user, date, and time for all database actions including selects, creates, modifies, and deletes. |
| 21 CFR § 11.70<br>Signature/Record Linking | All database activities can be recorded in Teradata Database's audit log. This includes the data required for an electronic signature. |
| 21 CFR § 11.100<br>Unique electronic signatures | N/A |
| 21 CFR § 11.200<br>Electronic signature components | Teradata Database requires users to provide a username and password to access the database. Security in the form of biometrics or hardware tokens can also be deployed in conjunction with external directories. |
| 21 CFR § 11.300(a)<br>Unique IDs/passwords | It is impossible for two individuals to have the same combined identification code within Teradata Database. |
| 21 CFR § 11.300(b)<br>Password aging | Teradata Database supports these password usage controls: password expiration, maximum logon attempts, locked user expiration, and password reuse restrictions. |
| 21 CFR § 11.300(c)<br>Loss management | Teradata Database can quickly disable accounts that have been compromised or are otherwise suspect. |
| 21 CFR § 11.300(d)<br>Transaction safeguards | Teradata Database has extensive audit capabilities that can be used to identify unauthorized access attempts. |
| 21 CFR § 11.300(e)<br>Testing of biometric devices | Through a variety of directory services, products, and other external authentication mechanisms, Teradata Database can make use of hardware tokens and cards that supply authentication credentials. |

Our initial third party audit was conducted by Science Applications International Corporation on June 20, 2007. While it's only one component of a complete Part 11 compliant solution, we recognize the importance of maintaining ongoing compliance of the Teradata Database on behalf of our life sciences customers. As such, IQ, OQ and PQ test scripts, developed by CIS as part of their 2015 audit, are executed against the final production version of the Teradata RDBMS for every major database upgrade.

The following chart contains information on historical and current script executions that ensure the most current major release of the Teradata database is in full compliance with and can support our customer's 21 CFR Part 11 requirements:

| Database Version | Scripts Executed | Result |
|---|---|---|
| Teradata 14.10 | July 10, 2015 | Successful |
| Teradata 16.10 | May 3, 2017 | Successful |

10000 Innovation Drive, Dayton, OH 45342 **Teradata.com**