

# Teradata Solutions

## Helping You on Your Journey to Part 11 Validation

Industry Solutions > Life Sciences

Today's biopharmaceutical labs and manufacturing operations demand robust applications to facilitate the discovery, refinement, and production of the latest miracle 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 addresses 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

The Teradata Database offers capabilities designed to address Part 11 requirements. These include:

#### Independently Verified Controls

Teradata has undergone a Common Criteria Evaluation that included rigorous testing of all its security controls by an independent Common Criteria Testing Lab.

#### Robust Authentication

Teradata implements strict login security controls ensuring that only authorized individuals can gain access to the database. These controls include password complexity restrictions, encrypted credential exchanges, and system identifiers that support native and external directory authentications, including Active Directory and standard LDAP implementations.

### Extensive Auditing Logging Capability

Teradata Database can log every database access including selects, writes, and deletes. Each event log entry contains the event date and time, the user identity and account, the event type and whether or not it was successful, the logical host from which the request originated, the session identifier, the initial logon data and time for the session, and the client in the form of the IP address.

### Separation of Duties

Teradata enables you to separate administrative duties so that each administrator can only perform limited functions based on appropriate authorization. It can enforce this separation of duties and check to ensure that users are permitted to execute the appropriate SQL statements based on highly granular access controls. For example, Teradata can implement database, table, and row level restrictions for selects, creates, modifies, and deletes.

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](http://Teradata.com).



## How Teradata Addresses Part 11 Requirements

While it's only one component of a complete Part 11 compliant solution, this table describes how Teradata Database can assist your company on your path to Part 11 validation.

Part 11 Requirement	The Teradata Approach
<b>21 CFR § 11.10(a) System validation</b>	Teradata Database has successfully undergone a Common Criteria evaluation, an intensive scrutiny of all security controls.
<b>21 CFR § 11.10(b) Accurate and complete copies of records</b>	Teradata Database ensures that all changes are documented and can hold individuals responsible for changes through extensive logging capabilities.
<b>21 CFR § 11.10(c) Protection of records</b>	Teradata Database can enforce strict rules with respect to retention. For example, permissions for select, create, modify, and delete can be assigned separately.
<b>21 CFR § 11.10(d) Limiting system access</b>	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.
<b>21 CFR § 11.10(e) Computer-generated audit trail</b>	Teradata Database can log each and every database access including selects, writes, and deletes.
<b>21 CFR § 11.10(f) Operational system checks</b>	Teradata Database can enforce separation of duties and check to ensure that users are permitted to execute the appropriate SQL statements.
<b>21 CFR § 11.10(g) Authority checks</b>	Teradata Database implements strict login security controls that ensure that only authorized individuals can gain access to the database.
<b>21 CFR § 11.10(h) Devices checks</b>	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.
<b>21 CFR § 11.10(i) Education and training of personnel</b>	The Teradata Database system comes with an extensive library of documentation to assist administrators and end users.
<b>21 CFR § 11.10(j) Personnel accountability</b>	The Teradata Security Administration manual provides guidance for sound security practices related to the security of the overall operating environment.
<b>21 CFR § 11.10(k) Control of documentation</b>	N/A
<b>21 CFR § 11.30 Controls for open systems</b>	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.
<b>21 CFR § 11.50 Signature Manifestations</b>	Teradata Database can record user, date, and time for all database actions including selects, creates, modifies, and deletes.
<b>21 CFR § 11.70 Signature/Record Linking</b>	All database activities can be recorded in Teradata Database's audit log. This includes the data required for an electronic signature.
<b>21 CFR § 11.100 Unique electronic signatures</b>	N/A
<b>21 CFR § 11.200 Electronic signature components</b>	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.
<b>21 CFR § 11.300(a) Unique IDs/passwords</b>	It is impossible for two individuals to have the same combined identification code within Teradata Database.
<b>21 CFR § 11.300(b) Password aging</b>	Teradata Database supports these password usage controls: password expiration, maximum logon attempts, locked user expiration, and password reuse restrictions.
<b>21 CFR § 11.300(c) Loss management</b>	Teradata Database can quickly disable accounts that have been compromised or are otherwise suspect.
<b>21 CFR § 11.300(d) Transaction safeguards</b>	Teradata Database has extensive audit capabilities that can be used to identify unauthorized access attempts.
<b>21 CFR § 11.300(e) Testing of biometric devices</b>	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.

Teradata and Teradata Corporation are registered trademarks of Teradata Corporation. Teradata continually improves products as new technologies and components become available. Teradata, therefore, reserves the right to change specifications without prior notice. All features, functions, and operations described herein may not be marketed in all parts of the world. Consult your Teradata representative or [Teradata.com](http://Teradata.com) for more information.

Copyright © 2007 by Teradata Corporation All Rights Reserved. Produced in U.S.A.

