Waters Empower 2 Software Seamlessly Manages Regulated Data to Aid in 21 CFR Part 11 Compliance
Summary

The objective of this white paper is to discuss the 21 CFR Part 11 compliance utility of Waters® Empower™ 2 Software for the regulated scientific laboratory. Regulated pharmaceutical and biotech arenas are currently striving to meet compliance with 21 CFR Part 11, the U.S. Food and Drug Administration’s (FDA) rule governing electronic records and electronic signatures.

Meeting Part 11 compliance remains challenging; eventually Part 11 will be viewed as a significant, impelling force to drive companies from a paper-records environment to a more efficient electronic-records environment. Although it’s understood that merely purchasing a chromatography data software package that incorporates thorough Part 11 technical controls does not make one fully compliant, complete technical controls should be inherent in any system that is used in a regulated environment. The technical controls for 21 CFR Part 11 compliance are built into Empower 2 Software.

21 CFR Part 11 Background

Regulations affecting the creation, maintenance, transmission, storage and modification of electronic records have recently added new focus to the regulated life science industries. 21 CFR Part 11, the FDA rule governing electronic records and electronic signatures, has emerged as among the most defining regulations for the pharmaceutical and biotech industries. The impact is far-reaching, affecting quality assurance, quality control, information technology, manufacturing, lab management and researchers’ practices. 21 CFR Part 11, currently in force as part of GxP inspections, has transformed the management of electronic data in regulated life science industries.

Part 11 has serious overall implications for all aspects of regulated enterprise operations. No one technology or discipline is more or less affected by the rule; it is pervasive throughout an organization. Every system that generates electronic records required by a predicate rule (GxP) must be examined to determine its current ability to comply with Part 11. Potentially, hundreds of systems within a pharmaceutical or biotech company may be affected. This includes analytical instruments (HPLC, UPLC™, GC, UV, MS, etc.) and Microsoft Office tools are currently being maintained by a variety of inconsistent methods that make it difficult to either retrieve or re-use this data in an expeditious and uniform manner.

Raw data is defined as an electronic record the minute it is saved to durable media. Metadata, or data about data, must also be saved and archived electronically. Since one cannot print to paper every bit of metadata available in electronic form, and since the FDA wants to use the same tools to evaluate the data the operator used, paper printouts are no longer a suitable substitute for electronic data. It is important that you maintain and protect the raw data, the metadata and the report data for each regulated system. Electronic records should not be deleted after they have been printed.

Empower 2 Software is designed to archive and catalog both the machine- and human-readable data allowing companies to:

• Become compliant with the FDA ruling on electronic records and electronic signatures
• Archive machine-readable data from any controlled instrument to safe, stable and secure media
• Retrieve machine-readable data on demand within minutes via an online storage device
• Establish traceability between the human-readable data and the machine-readable data
• Integrate Empower 2 Software with other applications
Summary of Waters Strategies for Compliance
Empower 2 Software uses Oracle as the underlying relational database, providing a robust and scalable architecture. Empower 2 Software meets all of the technical requirements for electronic records as prescribed by 21 CFR Part 11. The current version of this product helps any regulated company meet the core requirements of Part 11 with a clear plan and strategy for full compliance, including electronic signatures.

The following sections describe the key recommendations of Part 11 and how Empower 2 Software aids in compliance with the described technical controls.

SCOPE OF 21 CFR PART 11 (§ 11.1):

The general scope of Part 11 states, “The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.”

As the pharmaceutical and biotech industries move from paper to more flexible electronic data and information environments, Part 11 and other regulations will ensure continued data integrity in electronic formats. Overall, it is believed that more secure and trustworthy data will ultimately result from Part 11 compliance in the life science arena.

In addition to enhancing the integrity of data required to be maintained by the predicate rules (GxP regulates the Federal Food, Drug and Cosmetic Act, the Public Service Act or any FDA regulation except for Part 11), Part 11 also paves the way for full electronic submissions to the FDA.

The Rule says: “For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met…. For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part.”

Measures to ensure the trustworthiness of electronic records and electronic signatures consist of administrative, procedural and technical controls implemented for computer systems. This publication mainly focuses on the technical controls required by Part 11 that are provided by Empower 2 Software for trustworthy and reliable scientific data management.

Although this paper addresses key technical controls from 21 CFR Part 11, it is not intended to cover everything that Part 11 compliance should encompass. To satisfy this requirement, persons must, among other things, employ procedural and administrative controls that oversee conformance to Part 11 requirements.

Electronic Records—Applicability and Definition
Per 21 CFR Part 11, the definition of an electronic record is, “any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.”

21 CFR Part 11 applies to all electronic records used to meet GxP (GMP, GCP, GLP) requirements, including, but not limited to, systems for:

- Batch records, SOPs, test methods, specifications and policies
- Inventory records
- Calibration and preventative maintenance records
- Validation protocols and reports
- LIMS systems
- Chromatography data systems
- Customer-complaint files
- Adverse event reporting systems
- Automated document management systems

CONTROLS FOR CLOSED SYSTEMS (§ 11.10):

Essentially, these are the measures designed to ensure the integrity of system operations and electronic records stored in a closed system.

Section 11.3 indicates that a, “Closed System means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.” By definition, Empower 2 Software is a closed system.

The Rule further states that, “Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the
authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.”

Some of the procedures and controls required to maintain record integrity in closed systems include:

- Validation (§11.10(a))
- The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review and copying by the agency (§11.10(b))
- Protection of records to enable accurate and ready retrieval throughout the records retention period (§11.10c)
- Limiting system access to authorized individuals (§11.10(d))
- The use of computer generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation will be retained for a period as least as long as that required for the subject electronic records and will be available for agency review and copying (§11.10(e))
- Use of operational system checks to enforce permitted sequencing of steps and events (§11.10(f))
- Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record or perform the operation at hand (§11.10(g))
- Use of device checks to determine the validity of the source of data input or operational instruction

Let’s take a look at some of the Part 11 technical controls in more detail.

**ACCURATE AND COMPLETE COPIES:**

§11.10(b) of the Rule states that one must have the ability to generate accurate and complete copies of records.

The ability to make accurate and complete copies of data and metadata is very important. This is critical when considering that the FDA considers paper printouts of electronic records not suitable substitutes for those electronic records.

Archiving implies that electronic information is stored and then moved from active state to inactive state. Upon archiving, records must be protected to ensure record access and usability for the duration of the established record retention period. Controls must be implemented to ensure that archiving preserves the trusted status of the record and allows for long-term access and use.

Secure archiving requires:

- Moving data to a secure storage area that is still retrievable, in human-readable form
- Maintaining the integrity of the data during a move
- Validating the data move
- Maintaining data integrity for the duration as defined in applicable record retention policies
- Technology that preserves integrity of the record before, during and after a data migration activity
- Ensuring that the audit trail is archived
- Technology and procedures that permit data to be retrieved and copied, in both electronic and human readable form, throughout the life of the data

**AUTOMATED BACKUP OF LABORATORY DATA:**

Empower 2 Software captures both human-readable and machine-readable data accurately, electronically and automatically.

Empower 2 backup software automates the project backup process and provides a mechanism to backup several projects at one time. It also gives you the option to have your own backup software started automatically when Empower 2 is finished. You can easily retrieve backed up data by using the restore function, which allows you to restore one or multiple projects. It is also possible to either manually backup a project and samples, or schedule a back-up task using the Windows Scheduler.

Empower 2 Software dramatically reduces the amount of time required to properly manage the vast amount of data generated in labs every day. Analysts and lab managers can work with complete confidence that the data is being safely and securely backed up and can be easily accessed when required. No user intervention is required.
It is imperative to capture the corresponding metadata along with the electronic record. Empower 2 Software automatically backs up all the metadata from both raw data, and human-readable records in a project, and stores this with the files in a protected, closed environment.

The user can review a list of projects (Figure 1) that have been backed up.

The FDA’s intention is that you should be able to generate your original results from your original raw data. To do that, you not only need the raw data but also the metadata.

Since it uses a relational database, Empower 2 Software provides superior traceability of raw data to results, calibration curves, instrument methods, processing methods and sample sets. Empower 2 Software allows for immediate, but controlled, access to electronic data stored in its secure Oracle database.

PROTECTION AND READY RETRIEVAL OF RECORDS:

§11.10(c) of the Rule states that records must be protected to enable their accurate and ready retrieval throughout the records retention period. Records should be protected against the likes of uncontrolled modification or deletion, and the system should automatically recognize when records have been altered after the initial recording.

The system must also allow for accurate and ready retrieval of such records. Part 11 does not specify a timeframe for the retention period; retention time is defined by the predicate rules.
Empower 2 Software is designed to retain human-readable and machine-readable records for as long as the designated retention period states. The architecture of the system is based on an Oracle database with distributed components to support enterprise-wide deployment.

Waters technologies’ products provide the ability to achieve compliance with §11.10 of the Rule. All Empower 2 Software components are compliant ready with sub-sections 11.10 a-g.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.

For records protection, Empower 2 Software utilizes Privileges that defines users and user groups, and assigns privileges therein. For example, someone with pre-defined chemist privileges would only be allowed to sign reports for review, without the capability of approving them.

Accurate and complete copies of machine-readable data and metadata can be made using Empower 2 Software. Likewise, accurate and complete copies of human-readable data and metadata can be made using Empower 2 Software.

Empower 2 Software requires an authorized user login to gain access to the system. Once logged on, a privilege grid controls the user’s access to data. Empower 2 Software does not allow users to perform illegal actions within the system. Proper sequencing of steps and events is typically procedural and will vary greatly from site to site.
controlled by persons who are responsible for the content of electronic records that are on the system.”

It is further stated that, “Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.”

An example of such an open system is an unsecured, web-based system used for transmitting data. Subpart B, §11.30 states that the controls for closed systems also apply to open systems. However, in order to maintain the authenticity, integrity and confidentiality of electronic records that are transmitted over an open system, tighter controls such as digital encryption would be required. Empower 2 Software is not an open system.

Electronic Signatures—Applicability and Definition

Part 11 defines an electronic signature as, “a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature.”

Many companies are not ready for e-signatures, but must still comply with all of the regulations regarding electronic records. The FDA is permitting the use of a hybrid system for companies that maintain archives of the electronic versions of each record while concurrently using paper-based signature processes.

It is vital to be able to prove the identity of an individual required to sign an electronic record. The key is linking the owner to the electronic identity and confirming that the individual has the authority to sign.

**SIGNATURE MANIFESTATIONS (§ 11.50):**

21 CFR Part 11 does not mandate electronic signatures, nor does it mandate when an e-signature is used or what documents must be signed. This is governed by the predicate rules.

The Rule does, however, require signature manifestations to contain three key pieces of metadata. It is stated that “Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).”

Also, the electronic signature is subject to the same

![Figure 6. Above, an Empower 2 Software display of e-signature history. Note the display in human-readable form of the three pieces of metadata needed for an e-signature manifestation.](image)
controls as e-records and must be included in any human-readable form of the record such as display or printed copies.

Empower 2 Software provides the ability to achieve compliance with this part of the Rule. The software captures and displays the three pieces of metadata of which a signature manifestation should consist. The Empower 2 Software e-signature option displays the full printed name of the signer, the date and the time that the signature was executed and a meaning for the signature (configure meanings in the Project Manager for review, approval, authorship, responsibility, etc.). These are all required elements when a record is signed.

For trustworthy signed electronic records, electronic signatures should be unique to one individual and should not be reused or reassigned to anyone else:

- Empower 2 Software prevents re-allocation of e-signatures and prevents deletion of any information relating to a signature once it has been used
- Empower 2 Software does not allow signature information to be removed from an electronic record once it has been applied

**SIGNATURE/RECORD LINKING (§ 11.70):**

Section 11.70 ensures the integrity of either electronic or handwritten signatures executed to electronic records by specifying that, “Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.”

Linking the signature to the original electronic record is especially critical when a printout or an electronic copy of the e-record becomes orphaned from that e-record. The signature must not be lost.

Empower 2 Software provides the ability to achieve compliance with this part of the rule. The software enables non-breakable linking of electronic signatures to electronic records. The Empower 2 Software e-signature information is stored in the Oracle relational database and is permanently linked to the record itself. It is not possible to excise, copy or transfer the signature to another unsigned document.

**ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS (§ 11.200):**

Electronic signatures may be either non-biometric or biometric. For non-biometric electronic signatures, two forms of identification are required. These can be any of the following:

- User ID and password
- Card key and password
- Two passwords

The Rule defines Biometric as, “A method of verifying an individual’s identity based on measurement of the individual’s physical feature(s) or repeatable actions(s) where those features and/or actions are both unique to that individual and measurable.”

Some familiar examples include, voiceprints, finger/thumb print recognition, retinal scans or any device or method designed to ensure use only by the genuine owner.

“Electronic signatures that are not based upon biometrics shall:

1. Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each

![Figure 7](image-url)
signing shall be executed using all of the electronic signature components.

2. Be used only by their genuine owners; and

3. Be administered and executed to ensure that attempted use of an individual’s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.”

Non-biometric e-signatures must be administered and executed to prevent forging.

**ELECTRONIC SIGNATURES, GENERAL REQUIREMENTS (§ 11.100):**

“Electronic signatures not based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.”

Empower 2 Software:

- Provides the ability to achieve compliance with this part of the Rule
- Uses Oracle tools to manage user ID and password for e-signature manifestations

- Requires both components for all signatures; reason codes may be restricted to authorized users
- Requires a Username/Password combination in order to e-sign a report
- Further administrative and procedural controls are also required on the part of the user to ensure that passwords and user IDs are utilized and administered properly
- Biometric signatures are not included in Empower 2 Software; if biometrics are requested by customers, we will consider adding this feature in a future release

§11.200(a)(1) System shall ensure that the first signing in a controlled session requires both signature components.

- Within Empower 2 Software, each time you sign a report in a non-contiguous fashion, both the username and password are required for authentication
- During non-continuous access, both components are required for each signing. See §11.200(a)(1)

**CONTROLS FOR IDENTIFICATION CODES/ PASSWORDS (§ 11.300):**

Ultimately, the purpose of Part 11 is to achieve trusted electronic records. The identity of the user is essential to irrefutably label an individual responsible for some aspect of the electronic record. Electronic identification is the passive harvesting of users’ identities as they are performing tasks on a system.

Some characteristics of electronic identification include:

- Users typically assigned an ID as part of system.
  The ID is passively captured/harvested as the user operates the system
- If an electronic ID is collected, it must be linked to the record for the duration of the record
- Electronic ID does not have the same force of law as electronic signature; however, it still implies attributability and should be taken seriously

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity.

Such controls shall include:

A. Maintaining the uniqueness of each combined identification code and password, such that no
two individuals have the same combination of identification code and password.

B. Ensuring that identification code and password issuances are periodically checked, recalled or revised (e.g., to cover such events as password aging).

C. Following loss management procedures to electronically unauthorize lost, stolen, missing or otherwise potentially compromised tokens, cards and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

D. Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

E. Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

- Empower 2 Software provides the ability to achieve compliance with this part of the Rule.
- The software uses Oracle tools to manage user ID and password for e-signature manifestations.
- Sections 11.300 A, C and E above are the user’s responsibility; they fall under administrative/procedural controls.

§11.300(b) System should force password changes periodically

- Empower 2 Software allows an administrator to force a password change based upon company policy and business rules.

§11.300(d) Ability to notify administrators of unauthorized system access attempts and lock terminal after a specified number of failed attempts

- Empower 2 Software provides this capability through Oracle.
- In the event of more than a specified number of unsuccessful attempts to log in to Empower 2 Software, the following will occur:
  - The user account is disabled, requiring an administrator to unlock
  - Notification is sent to the Security Monitor and the Audit Trail
  - This feature cannot be disabled

Audit Trails

As mentioned previously, the use of computer-generated, time-stamped audit trails are a significant part of the ‘Controls for Closed Systems.’ (See 21 CFR Part 11 §11.10.) Even though an audit trail is nothing new for FDA regulated environments, it is the most frequently discussed requirement of Part 11, primarily due to the expected cost of upgrading legacy systems that lack complete audit trails.

Audit trails are considered the key to the security of a system since they track access to the data. In this way, an incomplete or absent audit trail can impact data integrity or even product quality. The absence of an audit trail is considered to be, “highly significant when there are data discrepancies” according to the FDA.

The benefits of having a complete audit trail irrespective of compliance include using it to deter fraudulent manipulation of records, detect device tampering by the device owner, alert administrators when investigation is necessary, maintain record integrity and reduce the risk of information being lost or changed.

Part 11 requires electronic audit trails for all data archived and managed as per the Rule. Audit trails must be:

- Operator independent — no operator may change, sign, write-to or modify in any way
- Computer generated (automatically)
- Include date and time the individual created, modified, reviewed, approved or deleted an electronic record
- Time and date stamped using local time in an unambiguous format (military or standard time)
- Secure — reasonable security to prevent tampering

The audit trail documentation must be retained for the same period as electronic record. Accurate and complete copies must be made available to the FDA for review and copying and must be both human-readable and machine-readable.

Additionally, the recorded changes must not obscure
previously recorded information, and any changes need to be documented in the audit trail.

Empower 2 Software and Project Audit Trails provide a history of actions that affects the System (such as denied login, project archival, changes to system policies). The Project Audit Trail captures information that affect the data within a project (calibration, method changes, processing data) and other information captured in the Empower 2 Software database (who, when, what) including any data insertions, modifications to metadata, record copies, deletions and template applications.

Empower 2 Software does not allow the data itself to be changed. Changes to user privileges are also tracked. The audit trails are generated automatically.

Empower 2 Software has the ability to discern invalid or altered records.

Empower 2 Software provides checksum and cyclic redundancy check (CRC) verification for all human-readable and machine-readable data to protect against data being altered within the system.

**Manage Validation and Compliance Documentation**

Empower 2 Software can be used to store qualification data for instruments and software in the lab. Since these checks need to be performed periodically, Empower 2 Software provides not only a convenient storage location, but also a way of clearly documenting the timing of the various qualification tests done in the lab. Validation and compliance documentation is immutably stored within the relational database.

**Beyond the Rule: Other Data Management Solutions from Waters Corporation**

**Assistance with Audits**

Auditors require objective evidence to be provided in a timely fashion. If analytical reports are online in the Empower 2 Software database, providing documented evidence becomes a fast, streamlined process. Empower 2 Software acts like an electronic filing cabinet. Instead of sifting through printed reports by hand, the Empower 2 Software view filters can directly access the requested report or reports.
Waters Laboratory Informatics

The Waters Laboratory Informatics suite, including Empower 2 Software, is made up of powerful, integrated information management solutions that enable you to compile, manage and share the vast quantity of data generated in your laboratory. Whether you’re searching for application-specific software or looking to augment your data management strategy, Waters Laboratory Informatics solutions transform raw data into your competitive advantage. Learn more at www.waters.com/informatics.

Waters Global Services

To achieve your greatest success, every aspect of your operation needs to work together. Waters Global Services creates programs that will optimize your entire laboratory and information management processes. We offer a comprehensive portfolio of services to help your laboratories perform at their best.

- **Instrument Services** extend and enhance the standard limited warranty you receive when you buy a Waters instrument, delivering the value you need to avoid costly and time-consuming system downtime.

- **Software Services** include enterprise implementation and validation services, training, and support programs for Waters Laboratory Informatics software products.

- **Professional Services** provide you with programs that improve laboratory productivity, including asset management, and relocation services.

- **Connections Compliance Services** provide you with timely and cost-effective solutions for your regulatory compliance challenges. Use Waters Compliance Services to verify proper equipment operation for cGMP/GLP compliance, significantly reducing operating costs.

- **Educational Services** provides extensive UPLC, HPLC, MS, and software training and education at your site, at our corporate headquarters or at our local offices around the world.

Waters Global Services’ worldwide service and support organization is staffed by experts in 94 offices located in more than 50 countries. Our technical experts are available in person, on the phone, or at www.waters.com to answer questions and provide you with service, support and information.