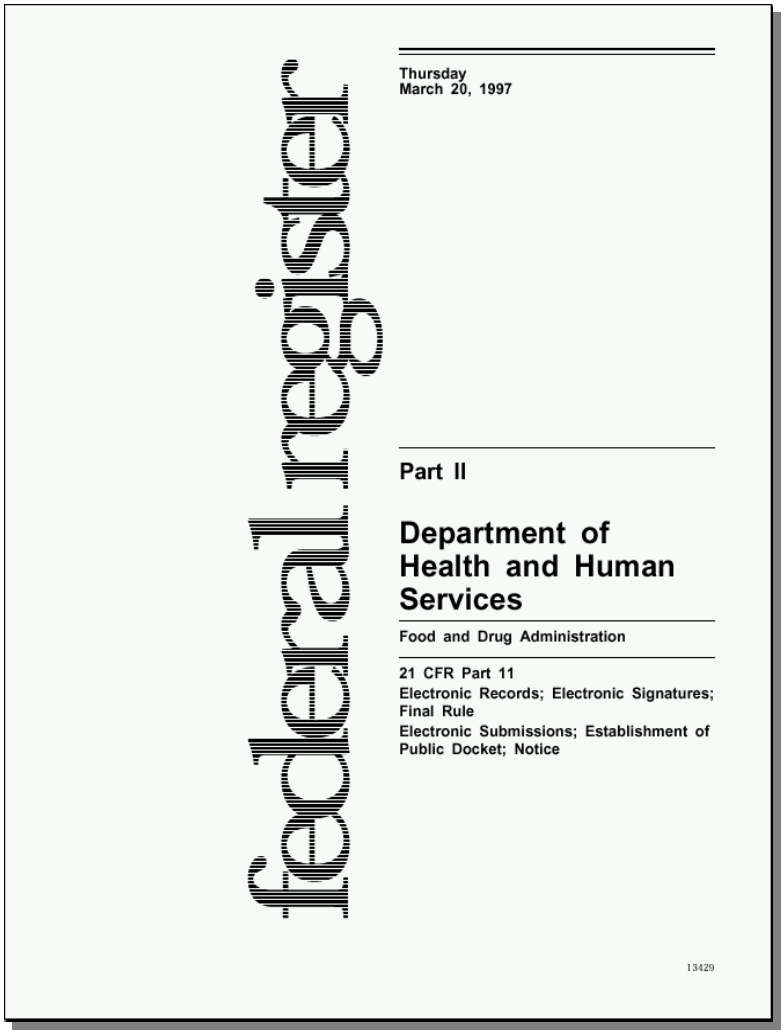
PerkinElmer Instruments
TotalChrom Client/Server

Achieving 21 CFR Part 11 Compliance with TotalChrom Client/Server Software



What is 21 CFR Part 11?

Title 21 of the Code of Federal Regulations (CFR) is the Section of the United States government Rules and Regulations document that deals with the Food and Drug Administration (FDA). Chapter I, Part 11 of this Section applies to records in electronic form and to the criteria under which the FDA will consider electronic records and signatures *"to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper".*

This final ruling, published on March 20, 1997 and in effect since August 20, 1997, is another step in the process of determining how to accommodate "paperless" record systems under the current *Good Manufacturing Practice* regulations of 21 CFR Parts 210 and 211. The ultimate goal is to provide the formal regulations for the submission of required documents to the agency [the FDA] in electronic format.

What is the purpose of this PerkinElmer document?

The purpose of this document is to describe the relevant portions of the 21 CFR Part 11 regulations and to explain their implementation using the **TotalChrom** Client/Server software.

It is critical to understand that such support is not entirely the responsibility of PerkinElmer and the **TotalChrom** software. As defined in the specifications of 21 CFR Part 11, it is also the responsibility of the persons using and implementing electronic records and electronic signatures to *"employ procedures and controls designed to ensure the authenticity, integrity and, when appropriate, the confidentiality of electronic records".*

Proper procedures and practices are as much a part of overall compliance with these regulations as are the features of the **TotalChrom** software. It is ultimately the customer's responsibility to implement and maintain, in a compliant manner, any data system generating electronic records.

1. Introduction

The PerkinElmer **TotalChrom** Client/Server system has been designed to perform chromatographic instrument control, data acquisition, data processing and reporting. In addition, **TotalChrom** supports a wide range of built-in features to provide FDA regulated organizations the capability to comply with the requirements detailed in 21 CFR Part 11. **TotalChrom** is designed to operate with the Microsoft Windows XP and Windows 2000 operating systems, providing users an even greater degree of security and access control. The combined functionality of the **TotalChrom** software and the security features of the Windows operating system together offer the tools required to implement a *technically* compliant chromatography data system (CDS).

It is important to recognize that "technical compliance", alone, does not fully satisfy the requirements of 21 CFR Part 11 to ensure "*the authenticity, integrity and confidentiality of electronic records*". It is also necessary to have in place suitable "procedural controls" that define the overall operation of the organization in which the CDS is used, consistent with the requirements of 21 CFR Part 11 and the "predicate rules" upon which it is based. For example:

> ***21 CFR Part 11, Subpart B—Electronic Records***
> ***Section 11.10 Controls for closed systems.***
>
> *(i)Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.*
>
> *(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.*
>
> *(k) Use of appropriate controls over systems documentation including:*
>
> > *(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.*
> >
> > *(2) Revision and change control procedures to maintain an audit trail that documents time sequenced development and modification of systems documentation.*

This PerkinElmer document is intended to provide a point-by-point response to the requirements indicated in 21 CFR Part 11, with respect to how **TotalChrom** technical controls can be implemented to address those points. Additional information is contained in the appendix of this document to assist in meeting more general cGMP requirements with **TotalChrom**. This appendix is designed only to provide further information to support the proper implementation of a **TotalChrom** system. It is not intended to be an authoritative guide to cGMP compliance.

2. Disclaimer

It is widely recognized that the ultimate responsibility for regulatory compliance rests with the customer. More explicitly, as stated in Section 11.10 of 21 CFR Part 11:

> *"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."*

In consideration of this, it must be understood and accepted that the information provided within this document is for guidance purposes only. PerkinElmer will not be responsible for citations or other customer compliance issues resulting from the inappropriate implementation or use of a TotalChrom system.

3. 21 CFR Part 11 – Final Rule

21 CFR Part 11	
Subpart A - General Provisions	
Section 11.1 Scope	
11.1 (a)	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.
11.1 (b)	This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.
11.1 (c)	Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically expected by regulation(s) effective on or after August 20, 1997.
11.1 (d)	Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.
11.1 (e)	Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.
Section 11.2 Implementation	
11.2 (a)	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.
11.2 (b)	For records submitted to the agency, persons may use electronic records in lieu of traditional signatures, in whole or in part, provide that: 1) The requirements of this part are met; and 2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must any accompany electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with electronic submission.
Section 11.3 Definitions	
11.3 (a)	The definitions and interpretations of terms contained in section 201 of the act apply directly to those terms when used in this part.
11.3 (b)	The following definitions of terms also apply to this part: 1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)). 2) *Agency* means the Food and Drug Administration. 3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable. 4) *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.

	5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. 6) *Electronic record* means 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. 7) *Electronic signature* means 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. 8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark. 9) *Open system* means an environment in which system access is not controlled by persons which are responsible for the content of electronic records that are on the system.

4. TotalChrom 21 CFR Part 11 Technical Compliance Matrix

Subpart B - Electronic Records		
Section 11.10 Controls for closed systems		
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	All projects within PerkinElmer Instruments follow a product development and management process, called **PACE,** that rigorously controls all phases of design, development, testing, documentation and support. In addition, software development is conducted in accordance with a Quality System following the guidelines of **GLP**, **GMP**, **GAMP**, **ISO 9001** and **TickIT,** and has been certified by the British Standards Institute (BSI). The PerkinElmer **TotalChrom** software has been developed using a version of the **GAMP** Software Development Life Cycle (SDLC) process, referred to as the "V" model. This process requires traceability between the ***Product Requirements Document (PRD)***, ***Functional Requirements Specification (FRS)***, ***Detailed Design Document (DDD)*** and Software Quality Assurance testing procedures. Document review and product testing are executed at various steps during the development phase, to match the requirements of the design documents against the features implemented in the code. Once a version of the product has been tested and released, GLP change control and document management procedures are followed to ensure continued traceability over the life of that product. Software "bugs" and feature enhancement requests are maintained in a Defect Management System. Cross-references to these entries are maintained in the Quality System documents as the bugs are corrected and the new features implemented. Review of these processes, procedures and documents can be conducted during a "Vendor Audit" of our facility in Shelton, Connecticut, USA. Access to product source code can be made available though a source code escrow service agreement. PerkinElmer also offers a complete package of products and services to assist the customer with the implementation and validation of a **TotalChrom** system. Installation Qualification **(IQ),** Operational Qualification **(OQ)** and Extended Operational Qualification **(EOQ)** services can be performed to document that the system has been properly installed and is operating according to PerkinElmer specifications. The formal Test Scripts used during the **TotalChrom** development and testing cycles can be made available to the customer to assist in their development of Performance Qualification **(PQ)** testing procedures. PerkinElmer can provide consulting services, as well, to assist in PQ development. To ensure the integrity of data in the system, all **TotalChrom** files are stored in a proprietary binary format. These files are further protected and made "tamper-resistant" and "tamper-evident" through the use of checksum auditing.
11.10 (b)	The ability to generate accurate and complete copies of records in both human readable and electronic formats suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such a review and copying of the electronic records.	**TotalChrom** has the ability to generate accurate and complete copies of its electronic records. Significant, formalized "stress testing" is conducted by the PerkinElmer Software Quality Assurance **(SQA)** department to demonstrate the reliability and integrity of such data generation. To ensure the integrity of data in the system, all **TotalChrom** files are stored in a proprietary binary format. These files are further protected and made "tamper-resistant" and "tamper-evident" through the use of checksum auditing.

		Data reports, as well as method and sequence listings, can be previewed on-screen or sent to a printer for hardcopy. Selected data files, methods, sequences, etc. can be copied for transfer to another system. These copied records will maintain their checksum values to ensure their integrity once moved to another system. Any attempt to modify a data file outside the **TotalChrom** operating environment will render that file invalid.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The **TotalChrom** operating environment provides protection of its electronic records as long as they are under its control. A combination of Windows Operating System security and application specific security features ensure that only authorized individuals have access to those records. As indicated above, **TotalChrom** electronic records, when copied or archived in their "native" format, use checksums to maintain their integrity once removed from the system. It is the ***customer's responsibility***, however, to develop and maintain procedures for routine backup of online data, Disaster Recovery and long-term archival storage.
11.10 (d)	Limiting system access to authorized individuals.	In addition to using the security of the Windows Operating System, **TotalChrom** provides a sophisticated and extremely granular mechanism for controlling user access to features, functions and data, through the use of "JobTypes" or function groups. These JobTypes can be configured to restrict access to any control in any dialog or on any form, as well as to disable any menu or sub-menu in the **TotalChrom** application. It must be noted, though, that this section (11.10) of 21 CFR Part 11 clearly 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.*" Beyond the technical compliance of the software to provide the necessary security features, it is still the ***responsibility of the customer*** to provide procedural controls suitable to implement the TotalChrom system in a compliant environment.
11.10 (e)	Use of secure, 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.	The **TotalChrom** application provides secure audit trail functionality to record the creation, modification and deletion of parameters within **TotalChrom** files. Windows Operating System functions are used to provide computer-generated audit trails for the creation, modification and deletion of the **TotalChrom** files themselves. The **TotalChrom** audit trail entries automatically indicate the record or records changed, the date and timestamp of the change, the full name and UserID of the operator making the change, and the previous value and the new value. The reason for each change can be configured for selection from a "reasons list", associated with the JobType of the user making the change. The reasons lists are configurable by the system administrator. The use of the reasons list can be "forced" by system configuration. In addition, a "free text" comment entry can be allowed. The audit trails for a **TotalChrom** record can be printed, displayed on screen or copied with their subject records for agency review. *It is the **responsibility of the customer** to implement and configure these audit trail features in a compliant manner.*
	Record changes shall not obscure previously recorded information.	Once an audit trail record is written, it cannot be deleted, modified, overwritten or otherwise obscured. When audit trailing is enabled, it cannot be bypassed or defeated.

	Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	The audit trail information is stored as part of the **TotalChrom** record to which it applies. It is inextricably linked to its subject record and will be retained as long as the record itself. These records are further protected and made "tamper-resistant and "tamper-evident" through the use of checksum auditing.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Where steps and events must proceed in a specific order, **TotalChrom** forces this order to be maintained. Deviation from the specified sequence of events is not possible. Similarly, if specific values or parameters must be set for the proper operation of a **TotalChrom** function, the software will not permit the operator to proceed until appropriate values are entered. "*Operational system checks*" do not preclude the customer from implementing procedural control over the system where customer defined steps and events are required in a specific order.
11.10 (g)	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.	A **TotalChrom** system can be configured to use the authentication of a Windows network Domain to control access to the **TotalChrom** application. In addition, **TotalChrom** provides a sophisticated and extremely granular mechanism for controlling user access to features, functions and data, through the use of "JobTypes" or function groups. These JobTypes can be configured to restrict access to any control in any dialog or on any form, as well as to disable any menu or sub-menu in the **TotalChrom** application. Beyond the technical compliance of the software to provide the necessary security features, it is still the ***responsibility of the customer*** to provide procedural controls suitable to implement the **TotalChrom** system in a compliant environment.
11.10 (h)	Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Manual data entry into a **TotalChrom** system can only occur through keyboard entry from the screens and forms of the application itself. All data entered in this way are checked, as appropriate, for valid data type and data ranges. Values inconsistent with this checking will not be permitted. Automatic data entry from a chromatographic instrument can only be received via PerkinElmer instrument interfaces configured for the system. Access to the instruments is controlled through **TotalChrom** JobType settings. As data are communicated between these interfaces and the **TotalChrom** acquisition computer, a checksum is applied to each data packet. If the checksum is not received, or if it fails, the data are re-transmitted until a successful transfer of that packet occurs. Data transmitted across a ***TCP/IP*** Local Area Network (LAN) are similarly protected against data loss or corruption.
11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	PerkinElmer offers an extensive range of end-user and system administrator training courses. These training courses can be provided in a standard format or tailored to meet the needs of the customer. All PerkinElmer employees involved with the development, support and maintenance of the **TotalChrom** software have been trained in GLP and 21 CFR Part 11 compliance.
11.10 (j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Beyond the technical compliance of the software to provide the necessary security features, it is still the responsibility of the customer to provide procedural controls suitable to implement the **TotalChrom** system in a compliant environment.

		As indicated in 21 CFR Part 11, Section 11.10: *"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."*
11.10 (k)	Use of appropriate controls over systems documentation including: 1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. 2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modifications of systems documentation.	All **TotalChrom** documents are maintained under strict control by the PerkinElmer SQA Department. SOPs are in place to govern revision, change control and general document management. These procedures have been developed to be consistent with those specified for record keeping and document management under GLP regulations. All documents are controlled through access restrictions. It is the ***responsibility of the customer*** to institute similar procedures for the control of **TotalChrom** system and user documentation.
Section 11.30 Controls for open systems		
11.30	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.	**TotalChrom** can be implemented in a compliant manner as either a closed or an open system. The definition of an "*Open System*", as described earlier, is, "*an environment in which system access is not controlled by persons which are responsible for the content of electronic records that are on the system.*" When a **TotalChrom** system is operated in an "*open*" environment, where system access is not controlled by persons responsible for the data, it is the ***responsibility of the customer*** to ensure that authenticity, integrity and confidentiality are maintained, beyond the controls of a "*closed*" system.
Section 11.50 Signature Manifestations		
11.50 (a)	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.	Electronic signatures in **TotalChrom** are associated with audit trailing events. All signed records include the full name and UserID of the signer, the date and time of the signing, and the meaning of the signature. The "meaning" can be configured for selection from a "reasons list", associated with the JobType of the signer. The reasons lists are configurable by the system administrator. The use of the reasons list can be "forced" by system configuration. In addition, a "free text" comment entry can be allowed. It is the ***responsibility of the customer*** to implement **TotalChrom** audit trails and electronic signatures in a compliant manner. It is also the responsibility of the customer "*to certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures*".
11.50 (b)	The items identified in paragraphs (a) (1), (a) (2) and (a) (3) of this section shall be subjected 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).	The integrity for the application and maintenance of electronic signatures is ensured by their association with the audit trail records to which the signatures apply. Each is inextricably linked to its subject record and will be retained as long as the record itself. The **TotalChrom** controls for audit trails are the same controls as those for electronic signatures. **TotalChrom** audit trails and electronic signatures can be included as part of any human readable form of the electronic record and will remain intact when those records are copied.

Section 11.70 Signature / Recording linking		
11.70	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.	The integrity for the application and maintenance of electronic signatures is ensured by their association with the audit trail record to which the signature applies. Electronic signatures are inextricably linked to their subject records. They cannot be excised, copied or otherwise transferred by ordinary means.
Subpart C Electronic Signatures		
Section 11.100 General Requirements		
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Electronic signatures in **TotalChrom** can be configured to force unique identification. Once an electronic signature has been assigned, it cannot be reused or reassigned.
11.100 (b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	This is a Procedural Control under the ***responsibility of the customer.***
11.100 (c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. 1) The certification shall be submitted in paper form and signed with a traditional signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. 2) Persons using electronic signature shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	This is a Procedural Control under the ***responsibility of the customer.***
Section 11.200 Electronic signature components and controls		
11.200 (a)	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 signing shall be executed using all of the electronic signature components.	**TotalChrom** does not use biometrics for electronic signatures. **TotalChrom** electronic signatures consist of a combination of a UserID and separate password. Electronic signatures are associated with modifications to **TotalChrom** electronic records. All such modifications are recorded in the audit trail for that subject record. The audit trail entries automatically indicate the record or records changed, the date and timestamp of the change, the full name and UserID of the operator making the change, and the previous value and the new value. When electronic signatures are enabled, the user is prompted for their UserID and password upon executing a **Save** command from the **TotalChrom** application. Each time a **Save** is executed, the user is prompted again to enter his or her electronic signature. The "reason" for each change and signature can be configured for selection from a "reasons list", associated with the JobType of the user. The reasons lists are configurable by the system administrator. The use of the reasons list can be "forced" by system configuration. In addition, a "free text" comment entry can be allowed.

		TotalChrom forces electronic signatures to be unique. They cannot be reused and they cannot be reassigned. Passwords for **TotalChrom** UserIDs can be configured as "pre-expired" so they MUST be changed upon initial login by the user. These features ensure that electronic signatures can be used only by their genuine owners, except through fraud.
	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 collaborations of two or more individuals.	It is the ***responsibility of the customer*** to ensure that the electronic signature feature of the **TotalChrom** software has been implemented in a compliant fashion. It is also the ***responsibility of the customer*** to have in place the appropriate procedural controls to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaborations of two or more individuals.
11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	**TotalChrom** does not use biometrics for electronic signatures. **TotalChrom** electronic signatures consist of a combination of a UserID and separate password.
Section 11.300 Controls for identification codes / passwords		
	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:	It is the ***responsibility of the customer*** to ensure that the electronic signature feature of the TotalChrom software has been implemented in a compliant fashion. It is also the ***responsibility of the customer*** to have in place the appropriate procedural controls to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaborations of two or more individuals.
11.300 (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.	**TotalChrom** forces electronic signatures to be unique. They cannot be reused and they cannot be reassigned. Passwords for **TotalChrom** UserIDs can be configured as "pre-expired" so they MUST be changed upon initial login by the user. These features ensure that electronic signatures will be unique and known only to their genuine owners.
11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as password aging).	**TotalChrom** password control for user accounts and electronic signatures is configurable by the system administrator. Settings can be configured for: • A minimum length of 1 to 40 characters (will not allow a succession of periods or spaces). • Non-reuse, so that the combination of UserID and password remains unique and cannot be transferred or used again. • Pre-expired, so they MUST be changed upon initial login by the user. • Passwords can be set expire from between 0 to 999 days. It is the ***responsibility of the customer*** to implement a suitable security strategy and procedural controls for the use of passwords in the **TotalChrom** system.
11.300 (c)	Following loss management procedures to electronically de-authorize 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.	**TotalChrom** can be used in conjunction with operating system security features to automatically disable a user account following a preset number of failed login attempts. It is the ***responsibility of the customer*** to implement a suitable security strategy and procedural controls for the use of passwords in the **TotalChrom** system.

11.300 (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.	**TotalChrom** provides an error log that records unsuccessful attempts to login to the application. The Windows XP and 2000 operating systems record failed login attempts in the system's security audit log. When authenticating **TotalChrom** users through the network domain, user accounts can be disabled after a set number of failed login attempts.
11.300 (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.	Such devices and device controls are the ***responsibility of the customer.***

5. Appendix: Current Good Manufacturing Practice (cGMP) - Guidance for TotalChrom Users

5.1. Principles

The principles underlying the need for and use of 21 CFR Part 11 are primarily, ***21 CFR Part 210 and 210 Current Good Manufacturing Practice*** and ***21 CFR Part 820 Quality System Regulation.*** It is a Quality System, as described in these *"Predicate Rules"*, which should be followed to ensure a compliant implementation of a **TotalChrom** system. The use of **TotalChrom** to record chromatographic data does not minimize the need to observe Current Good Manufacturing Practices for the operation of the system and the treatment of that data.

5.2. Validation

Before any data system can be put into use for routine or "production" work, an extensive amount of testing of that system, through the process of validation, must be performed. Validation is the process of establishing documented evidence that a system, process, procedure, equipment or mechanism is performing as it is intended to, based upon a detailed system design developed before the system is implemented.

The FDA ***Quality System Regulation, 21 CFR Part 820***, defines validation as follows:

> **Subpart A--General Provisions**
>
> **Section 820.3 Definitions.**
>
> *(z) Validation means confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use can be consistently fulfilled.*
>
> > *(1) Process validation means establishing by objective evidence that a process consistently produces a result or product meeting its predetermined specifications.*
> >
> > *(2) Design validation means establishing by objective evidence that device specifications conform with user needs and intended use(s).*
> >
> > > *(aa) Verification means confirmation by examination and provision of objective evidence that specified requirements have been fulfilled.*

Much of what is required for validation is derived from the following document:

> **21 CFR Part 211**
> **CURRENT GOOD MANUFACTURING PRACTICE FOR FINISHED PHARMACEUTICALS**
>
> **Subpart D-Equipment**
>
> **§ 211.68 Automatic, mechanical, and electronic equipment**.
>
> *(a) Automatic, mechanical, or electronic equipment or other types of equipment, including computers, or related systems that will perform a function satisfactorily, may be used in the manufacture, processing, packing, and holding of a drug product. If such equipment is so used, it shall be routinely calibrated, inspected, or checked according to a written program designed to assure proper performance. Written records of those calibration checks and inspections shall be maintained.*
>
> *(b) Appropriate controls shall be exercised over computer or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel. Input to and output from the computer or related system of formulas or other records or data shall be checked for accuracy. The degree and frequency of input/output verification shall be based on the complexity and reliability of the computer or related system. A backup file of data entered into the computer or related*

> *system shall be maintained except where certain data, such as calculations performed in connection with laboratory analysis, are eliminated by computerization or other automated processes. In such instances a written record of the program shall be maintained along with appropriate validation data. Hard copy or alternative systems, such as duplicates, tapes, or microfilm, designed to assure that backup data are exact and complete and that it is secure from alteration, inadvertent erasures, or loss shall be maintained.*

Validation must take into consideration specification, programming, testing, commissioning, documentation, operation, monitoring and modifying. This complete process is formalized in a *Validation Project Plan*. The Validation Plan includes, but is not limited to, specifications such as *Installation Qualification (IQ), Operational Qualification (OQ) and Performance Qualification (PQ).* These are defined in the FDA document ***Glossary of Computerized System and Software Development Terminology,*** dated August 1995, as follows:

> ***qualification, installation.*** *(FDA) Establishing confidence that process equipment and ancillary systems are compliant with appropriate codes and approved design intentions, and that manufacturer's recommendations are suitably considered.*
>
> ***qualification, operational.*** *(FDA) Establishing confidence that process equipment and sub-systems are capable of consistently operating within established limits and tolerances.*
>
> ***qualification, process performance.*** *(FDA) Establishing confidence that the process is effective and reproducible.*
>
> ***qualification, product performance.*** *(FDA) Establishing confidence through appropriate testing that the finished product produced by a specified process meets all release requirements for functionality and safety.*

More specific details for the expectation of software validation can be found in the document ***General Principles of Software Validation; Final Guidance for Industry and FDA Staff***, issued on January 11, 2002. An additional draft document ***Guidance for Industry, 21 CFR Part 11, Electronic Records; Electronic Signatures, Validation*** is also available from the FDA.

To satisfy the requirements for being "validatable", the **TotalChrom** software has been designed, developed and structurally validated following a *Certified Quality System* conforming to **GLP**, **GMP**, **GAMP**, and **ISO 9001**/**TickIT** guidelines. The software has been extensively tested by the PerkinElmer Software Quality Assurance (SQA) department, to document its performance in accordance with the design specification documents used within our Quality System. A review of these systems, processes and documents can be arranged through an on-site "vendor audit" at our facility in Shelton, Connecticut, USA.

PerkinElmer also offers formal, documented *Installation Qualification* (IQ) and *Operational Qualification* (OQ) services designed to assure the validity of the installation and primary operational ability of the system, in accordance with our specifications. A set of *Extended Operational Qualification* tests (EOQ) are also available. Completion of the *Performance Qualification* (PQ) for system validation is the ultimate responsibility of the customer and cannot be conducted by PerkinElmer due to the potential for a conflict of interest as the supplier of the software. However, PerkinElmer does offer the complete, formal suite of tests executed by our SQA department in the internal qualification of the software, as the basis from which final customer PQ testing design procedures can be developed. PerkinElmer can act as a consultant in this final phase of implementation testing.

5.3. Personnel Qualification

The following excerpts have been taken from the indicated FDA documents to stress the need and importance of adequately training users and system administrators in the proper operation of a **TotalChrom** system.

> **21 CFR Part 211**
>
> **CURRENT GOOD MANUFACTURING PRACTICE FOR FINISHED PHARMACEUTICALS**

§ 211.25 Personnel qualifications.

(a) Each person engaged in the manufacture, processing, packing, or holding of a drug product shall have education, training, and experience, or any combination thereof, to enable that person to perform the assigned functions. Training shall be in the particular operations that the employee performs and in current good manufacturing practice (including the current good manufacturing practice regulations in this chapter and written procedures required by these regulations) as they relate to the employee's functions. Training in current good manufacturing practice shall be conducted by qualified individuals on a continuing basis and with sufficient frequency to assure that employees remain familiar with CGMP requirements applicable to them.

(b) Each person responsible for supervising the manufacture, processing, packing, or holding of a drug product shall have the education, training, and experience, or any combination thereof, to perform assigned functions in such a manner as to provide assurance that the drug product has the safety, identity, strength, quality, and purity that it purports or is represented to possess.

21 CFR Part 820

QUALITY SYSTEM REGULATION

Subpart B--Quality System Requirements

Sec. 820.20 Management responsibility.

(b) (2) Resources. Each manufacturer shall provide adequate resources, including the assignment of trained personnel, for management, performance of work, and assessment activities, including internal quality audits, to meet the requirements of this part.

Sec. 820.25 Personnel.

(a) General. Each manufacturer shall have sufficient personnel with the necessary education, background, training, and experience to assure that all activities required by this part are correctly performed.

(b) Training. Each manufacturer shall establish procedures for identifying training needs and ensure that all personnel are trained to adequately perform their assigned responsibilities. Training shall be documented.

To achieve the level of training implied in these regulations, there must be close cooperation between those responsible for operating the system (*the users*) and those responsible for maintaining it (*the administrators*). A critical portion of system validation, *Performance Verification*, or *PQ*, is documentation that the system performs in the manner in which it was intended. Conflicting interests between the needs of the laboratory and the policies of an Information Technology (IT) Department can often compromise the intended performance of the laboratory system. To provide a comprehensive understanding of the requirements for the proper implementation of a compliant **TotalChrom** system, PerkinElmer offers a range of courses for all levels of personnel, and can customize these courses as needed to suit the specific requirements of the customer. All training materials and certificates are included with each course. Since an on-going level of vendor expertise must be made available to support a "production system", PerkinElmer also offers an Annual Software Support Contract to provide this service.

5.4. System Use and Operating Procedures

To ensure that the implementation and operation of the **TotalChrom** software is appropriate to meet the requirements of 21 CFR Part 11, GLP and GMP, considerations for the following procedures must be made. Many users find that such procedures form a suite of Standard Operating Procedures covering the various aspects of **TotalChrom** use.

- The server and client computers should be maintained in a suitable operating environment with ***appropriate security policies*** for their accessibility and use.

- A ***system document*** must be prepared to describe the physical and logical layout of the system, as well as the application configuration and user accounts. Diagrams are very helpful in designing, describing and aiding in troubleshooting.
- Standard Operating Procedures must be in place to define ***system access control and security features***, ***system management*** and ***general system operation***. These are generally separate procedures.
- ***Multiple levels of system access***, usually three or more, must be configured in the **TotalChrom** system through the use of the "JobType" functionality in the system administration level. JobTypes provide the ability to restrict access to any feature on any screen of the software, as well as to any menu or sub-menu throughout the system. Several example JobTypes, *Manager*, *UserA*, *UserB*, *UserC* and *KickOff*, have been provided as guides for developing ones more suitable to customer operations.
- The ***audit trailing features*** of the **TotalChrom** software must be enabled and appropriately configured. These audit trails are required to contain details of who made the change, when and why. Use the **TotalChrom** pre-defined "reasons for change" to provide users a list of authorized reasons from which to choose. Use the free text comments to record deviations and addition notes.
- There must be a ***procedure for data review***. In places where manual data entry is used, the entries should be checked and the results verified prior to data release. This may be, in part, covered through the validation of the **TotalChrom** software and specific chromatographic reports. However, following GLP guidelines for data review, second operator checking is generally the best approach to assure the accuracy of sample weights, standard amounts, dilutions, etc.
- Data must be secured against willful or accidental damage from either physical or electronic means. ***Validated backup and restore procedures*** must be developed and implemented on a routinely scheduled basis. One of the most common features of system security is to disable the "delete" permission for files and directories in the operating system of the computer. However, since system administrator accounts generally require the ability to delete files, there must be strict ***file deletion procedures*** in place and they must be followed rigorously. As further protection, it is highly recommended to enable the Windows XP or Windows 2000 ***operating system audit log*** to track general file creation, modification and deletion activity.
- ***A Disaster Recovery procedure*** must be in place to allow the continuation of operation in the event of a general system breakdown. Disaster recovery must be a tested and validated process with thorough documentation demonstrating the efficacy of the restoration process. It is recommended that a risk analysis be performed on the **TotalChrom** system to highlight areas of potential system weakness such as network switches and hubs, single server scenarios etc.
- A procedure must be in place to define the ***long-term storage of archival data***, generally to be maintained for the *Records Retention* period of the drug product and associated batch records. Such a procedure usually involves multiple, off-site copies of archived data, as well consideration for conversion of data to a "common" format, such as XML, that can be read in the future. An alternative to data conversion is a plan for maintaining a "legacy" system suitable for retrieving the archived data at some point in the future.
- Any potential changes to the validated **TotalChrom** system, such as software upgrades or computer hardware changes, must first be evaluated, tested and documented before being put into production. These processes for how changes are to be implemented must be described in a ***Change Control procedure***.
- When PerkinElmer or another outside agency is contracted to provide services affecting a validated **TotalChrom** system, the customer must ensure that there is a formal agreement in place to include a clear ***statement of the responsibilities*** delegated to the representative of that organization.

5.5. Summary

As stated earlier, it must be understood that the ultimate responsibility for operating a **TotalChrom** system in a compliant manner rests with the users of that system. The application of a **TotalChrom** Client/Server system within the pharmaceutical industry is considered acceptable for 21 CFR Part 11 compliance, provided the functionality and security controls detailed in this document are applied and the principles of cGMP are not compromised.

