

Using Chromeleon Chromatography Management Software to Comply with 21 CFR Part 11

The Electronic Records and Signatures Rule 1, known as 21 CFR Part 11, was established by the U.S. Food and Drug Administration (FDA) to define requirements for the use of electronic documents in lieu of paper records. The law was published in the Federal Register on March 20, 1997 and has been in effect since August 20, 1997. It specifies the system elements, controls, and procedures necessary to ensure the validity of electronically stored records. To aid in the determination of how the rule applies to each situation, the FDA has also issued a number of guidance documents that can be found at the FDA website².

Compliance with the law requires a combination of electronic systems and user-implemented procedural controls; no product or software alone can guarantee compliance. However, products with integrated functions that explicitly fulfill 21 CFR Part 11 requirements can significantly ease the task of achieving and maintaining full compliance with the law.

This Technical Note lists each relevant section of 21 CFR Part 11, and describes in detail how the Dionex Chromeleon[®] chromatography management system facilitates compliance.

Now sold under the
Thermo Scientific brand

Thermo
SCIENTIFIC

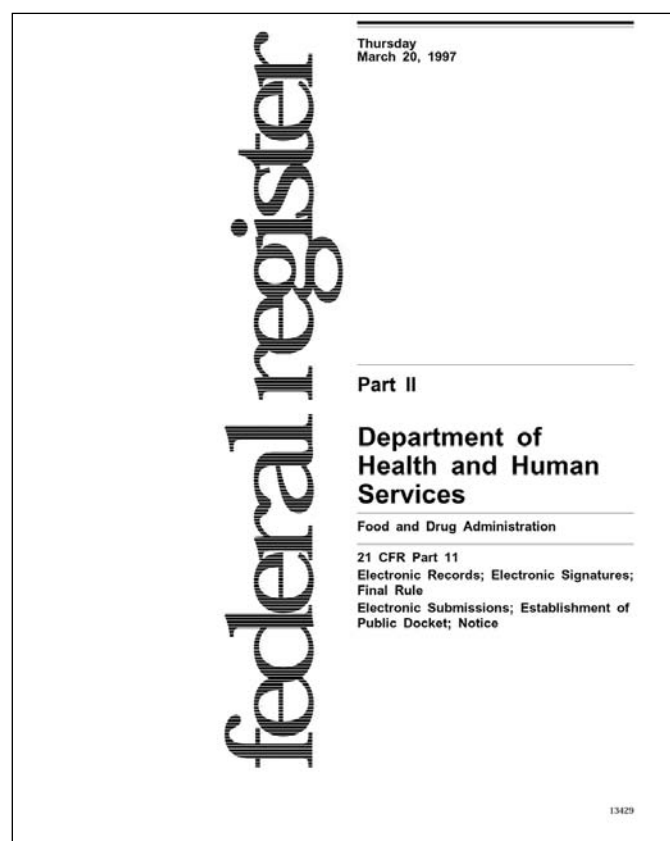


TABLE OF CONTENTS

	21 CFR section	Description	Federal Register Page	TN Page
Subpart A	11.1	Scope	13464	3
(General Provisions)	11.2	Implementation	13465	4
	11.3	Definitions		5
Subpart B	11.10 a	System Validation		7
(Electronic Records)	11.10 b	Copy Generation		9
	11.10 c	Record Protection		9
	11.10 d	Restricting Access		9
	11.10 e	Audit-trail generation		14
	11.10 f	Sequence enforcement		17
	11.10 g	Authority checks		19
	11.10 h	Device checks		19
	11.10 i	Training		20
	11.10	Documentation		20
	11.50	Signature Manifestations	13466	20
	11.70	Signature/Record linking		24
Subpart C	11.100	General Requirements		25
(Electronic Signatures)	11.200	Components and controls		26
	11.300	ID codes/password controls		27

SUBPART A— GENERAL PROVISIONS

§11.1 Scope

- (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.
- (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.
- (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 excepted by regulation(s) effective on or after August 20, 1997.
- (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.
- (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.

GENERAL PROVISIONS

Scope

21 CFR Part 11 pertains to all electronic records that are created, modified, maintained, archived, retrieved, or transmitted under FDA regulations (Subpart A Section 11.1b). The Scope and Application Guidance Document³ issued by the FDA clarifies this further, stating that Part 11 applies only in cases where electronic records are replacing paper records. The use of computer systems to generate paper records does not require submitters to follow this rule.

The electronic records of Chromeleon are discussed in detail under the Definitions section (see page 5). Because all electronic systems that are used with these records are required to have complete documentation available for FDA inspections, each Chromeleon shipment provides detailed user documentation, certificates of software validation, and SOPs for on-site system validation. Dionex stores copies of all versions of its software project documentation and source code in multiple secure locations, including a fireproof vault. This documentation includes product requirements, product specifications, design specifications, project schedules, test plans, test results, and validation documentation. All of these documents are produced for every release per the Dionex Design Control Procedure, which has been registered to ISO 9001 and is periodically audited. All Dionex documents and source code are available for inspection by the FDA at Dionex facilities.

To be prepared for a possible FDA audit, customers need to retain the following documents at their

CHROMELEON®
Version 6.80

Certificate of Software Validation

CHROMELEON Version 6.80 software and any related Service Packs have been designed, tested, validated and distributed according to Dionex Software Development Cycle guidelines modeled after ISO 9001:2000 standards. Structural and functional testing has also been done in accordance with these guidelines. Version 6.80 and any related Service Packs for Version 6.80 have met all functional specifications and release requirements. For public release, the protocol for changing Dionex software products includes documentation of the release and the archiving of source code in a secure location.

Version 6.80 and any related Service Pack Release Notes are provided with the software.

If required for detailed review by authorized governmental or regulatory representatives, Dionex provides confidential access to source code at Dionex's development facilities, along with access to documents and reports related to Dionex software products. A standard non-disclosure agreement may be required. All documents remain within the possession of Dionex Corporation at all times.

Der-Min Fun
Der-Min Fun
Manager, Software Engineering
Dionex Corporation

Klaus Rohm
Klaus Rohm,
Director, HPLC Hardware
And Software Engineering
Dionex Softron GmbH

Rebecca Ramos
Rebecca Ramos,
Quality Systems,
Dionex Corporation

Product Name: CHROMELEON
Version: 6.80

ISO 9001

DIONEX

Dionex Corporation, 1228 Titan Way, P.O. Box 3600, Sunnyvale, CA 94088-3600 doc.065130-01 Designed, developed, and manufactured under an NSFAT registered ISO 9001 Quality System

Figure 1. Certificate of Software Validation.

facilities:

- Certificate of Software Validation (Figure 1), which is included on the software media
- Completed Installation Qualification (IQ) records (blank forms and procedures for the hardware installation are shipped with the software; the software automatically performs software IQ tests to verify that program files are correctly installed, and stores the results on the system)
- Operational Qualification (OQ) and Performance Qualification (PQ) records for the systems and methodologies used (Chromeleon includes utilities and report forms that help laboratories standardize and automate the OQ and PQ tests)
- Site-specific standard operating procedures for security and records management

SUBPART A— GENERAL PROVISIONS

§11.2 Implementation

- (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.
- (b) 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, provided 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 accompany any 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 the electronic submission.

IMPLEMENTATION

Chromeleon produces electronically sealed reports, which are protected together with their root data. Chromeleon users can easily export copies of electronic records in Portable Document Format (PDF) for submis-

sion to agency units, in accordance with FDA guidelines.² The PDF files faithfully preserve the contents and formatting of the Chromeleon reports (Figure 2), including fields that list the people who electronically signed the records.

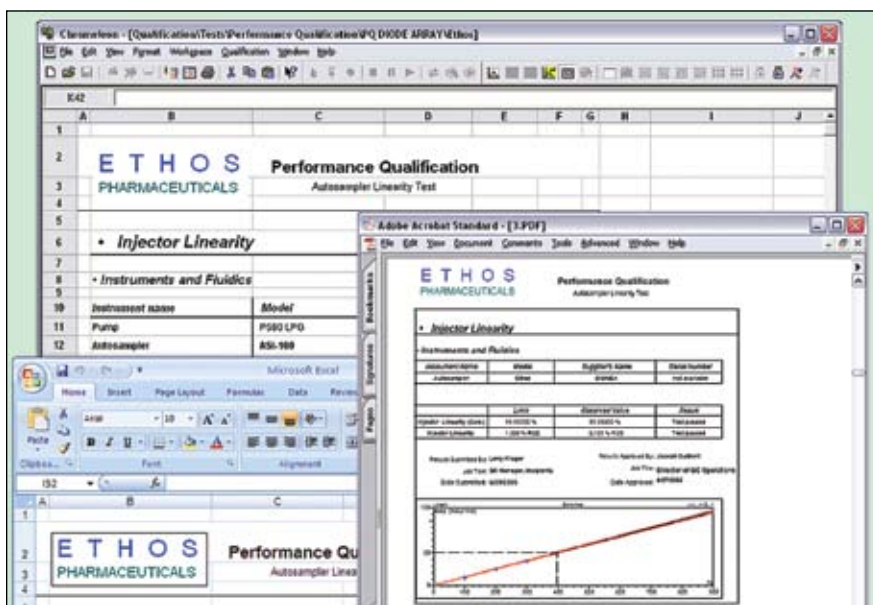


Figure 2. Chromeleon's reports can be exported as PDF files for convenient submission of results to regulatory agencies, and as XLS files for convenient collation with other tabular data.

**SUBPART A—
GENERAL PROVISIONS**

§11.3 Definitions

- (a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.
- (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 who are responsible for the content of electronic records that are on the system.

DEFINITIONS

Chromeleon is normally implemented in a closed-system environment, where the persons responsible for the records control access to the system. These persons include system administrators, who set up and maintain user accounts, plus any others (such as laboratory managers) who are granted privileges to control access to locations where Chromeleon data are stored. Chromeleon's security system supplements the security systems of the chosen operating system and relational database management software by providing control over specific chromatography-related resources and operations, not just system files and database records.

With respect to 21 CFR 11, the primary electronic records in Chromeleon are the injection sequences. Each sequence has all of the information

pertaining to the analysis of a set of samples (Figure 3). A typical sample set includes calibration standards, validation standards, blank injections, and unknowns. Included with each sequence are the following items:

- Sample information (sample names, sample IDs, sequence information, method assignments, correction factors, comments, user-defined sequence fields)
- Method information (instrument control programs, quantification methods, spectral libraries)
- Detector data (chromatograms, diode array data sets, mass-spectral data)
- Report templates (report definition files)
- Electronically signed reports
- Audit trails (system logs, modification histories, and electronic signature information)

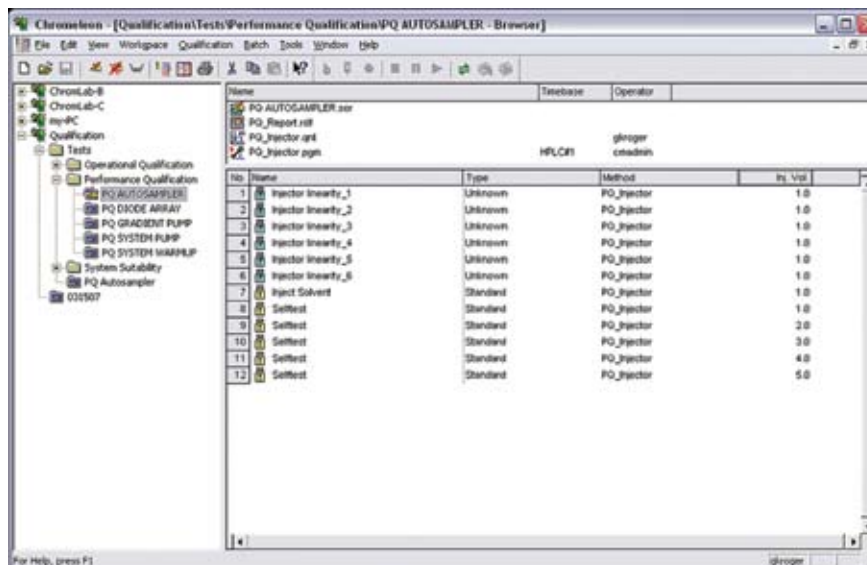


Figure 3. Sequences, represented by blue folders in the data browser, are Chromeleon's primary electronic records.

Chromeleon calculates results dynamically, so reports update instantly as new data are included or method settings are modified. This dynamic updating prevents inconsistencies between the implemented settings and the reported data. Modifications are permitted only prior to the application of electronic signatures, and audit trails keep track of all modifications, as described below. The operator initiates the electronic signoff process (discussed in the Signature Manifestations section) by submitting results for approval. Before the operator's elec-

tronic signature is applied, all source data and settings required to produce the report are automatically locked, and a hash code is calculated using the report contents, the operator's identification, and the current date and time. The operator is presented with a preview of the finished report, then prompted to enter his or her signature password. Upon entry of the password, an unalterable copy of the report is stored, along with the hash code needed to verify its authenticity. A similar process is followed by the reviewer (if any) and the approver of

the submitted report. If changes to the source data or report are needed, the signatures must first be removed by an appropriate authority.

Chromeleon can also generate backup files of the electronic records cited above, for data recovery and/or archiving purposes. Contents of backup files cannot be accessed outside of Chromeleon; the contents of a backup must be restored into the system before they can be read. Chromeleon's Modification History keeps track of all backup and restore operations.

SUBPART B— ELECTRONIC RECORDS

§11.10 Controls for closed systems

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. Such procedures and controls shall include the following:

- (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

CONTROLS FOR CLOSED SYSTEMS: VALIDATION OF SYSTEMS

The consistently accurate and reliable performance of workstations and instruments can be checked using Dionex AutoQ: a full suite of user-friendly, labor-minimized qualification tools. Included in AutoQ are the standard validation methods of installation qualification (IQ) and operational qualification (OQ) of instruments and software, as well as ongoing instrument performance qualification (PQ).

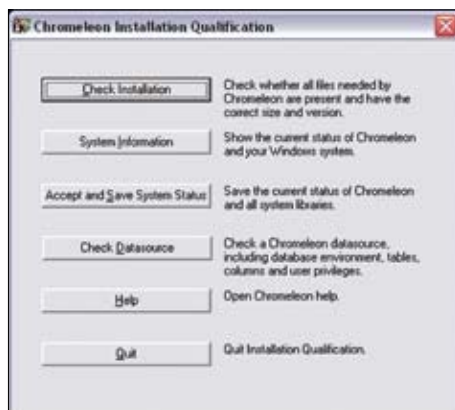


Figure 4. Chromeleon's integrated validation tools, such as the Software Installation Qualification, standardize and automate validation tests.

IQ is automatically performed on the software at installation, checking the correct structure of the installation and any shared files and drivers that are needed. A full report is produced and saved, listing any warnings or errors. Verification can also be performed later through a simple menu command (Figure 4). Another command runs the Chromeleon OQ, which generates reports using a standard data set to verify that the output is reproducible.

OQ and PQ of the entire system are easily performed using Chromeleon's qualification wizards, which automate the setup of sequences and generation of reports for qualification tests (Figure 5). They include checks for many important instrument parameters like gradient and flow precision, detector linearity, noise and drift, and injector linearity. In addition, to simplify the task of performing OQ and PQ tests, these tools ensure that all users perform the qualification tests consistently and in compliance with SOPs. The full suite of Dionex IC and HPLC systems can be checked, along with a number of third-party instruments. (See Chromeleon Help for details.)

Sample Name	Ret. Time min Uracil	Area mAU*min Uracil
injector linearity_1	0.500	2.481
injector linearity_2	0.500	2.482
injector linearity_3	0.500	2.481
injector linearity_4	0.500	2.473
injector linearity_5	0.500	2.496
injector linearity_6	0.500	2.496
Average:	0.500	2.487
RSD:	0.000 %	0.385 %
Limit:	0.500 %	0.500 %
Result:	ok	ok

Figure 5. Chromeleon's Performance Qualification reports provide detailed analysis of the performance of each component of the chromatography system.

The ongoing consistency of system and method performance can be monitored automatically during sample analysis via System Suitability tests. A wizard makes it easy to select common peak quality and reproducibility tests, or configure any number of custom tests using almost any reportable variable (Figure 6). Tests can be done on one or more individual injections, or span across multiple injections.

Chromeleon's Modification History (discussed in detail in the Audit Trail section starting on page 14), tracks all changes made to all data objects within the application. The Modification History lists, for each event, the time, date, affected data object, user ID, comments, and both the prior and current states of changed variables or entries. In Chromeleon's reports, any peak that has been manually manipulated is automatically flagged with an asterisk (Figure 7).

Data corruptions due to defects or failure of storage devices or media, or deliberate attempts to modify signed records, are detected and reported by Chromeleon. (See the Signature/Record Linking section.)

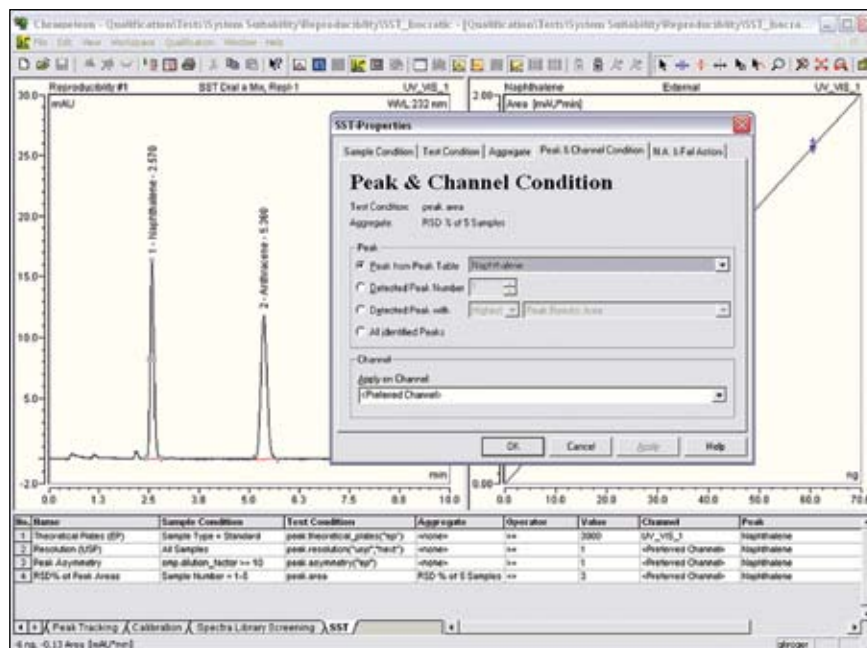


Figure 6. Any combination of System Suitability tests can be defined for any method to verify system performance during sample analyses.

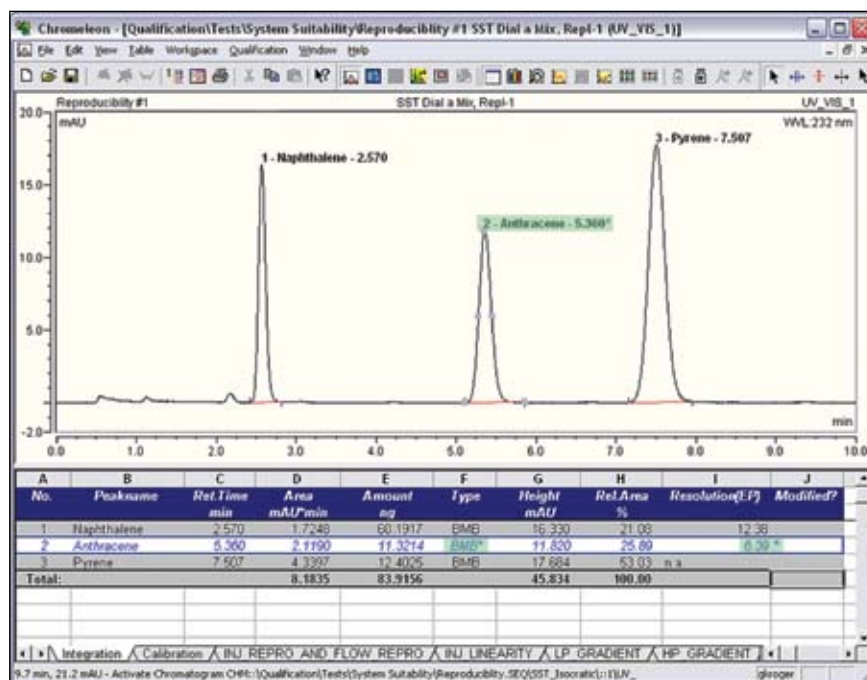


Figure 7. Chromeleon clearly indicates when a peak's integration has been modified.

**SUBPART B—
ELECTRONIC RECORDS**

**§11.10 Controls for closed systems
(continued)**

- (b) 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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.
- (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

**CONTROLS FOR CLOSED SYSTEMS:
GENERATION OF COPIES**

Chromeleon provides complete functionality for locating and viewing the electronic records on the system, and for generating complete, accurate paper and electronic copies for agency submissions. Printed copies include time/date stamps to facilitate traceability of paper documents. Electronic copies are produced in Portable Document Format (PDF) per agency guidelines, as discussed above.

**CONTROLS FOR CLOSED SYSTEMS:
PROTECTION OF RECORDS**

Chromeleon provides several layers of protection to ensure that accurate records can be readily retrieved.

The foundation for record protection is a secure operating system that provides positive user tracking and prevents unauthorized access to computers and files. Dionex recommends the use of Microsoft® Windows with the NTFS file system.

The next layer of protection is a secure relational database platform, which ensures that even those users who have access to files at the operating system level cannot read or modify records through means outside the secured application. Dionex recommends the use of Oracle® or Microsoft SQL Server as the relational database platform for secured, multi-user environments.

Beyond the protections afforded by the operating system and database platform, Chromeleon provides a comprehensive, chromatography-oriented security system that controls access to data, described further in the Restricting Access section. This ensures that only authorized users are able to access records and make changes; any such changes are

tracked by computer-generated audit trails, as described in the Audit Trail Section.

Records can be electronically signed, which simultaneously locks them and documents the signing authority, as described in the Signature Manifestations Section.

Replacement of items that have not been signed off can be either allowed or disallowed by the system administrator. If replacement is allowed, the Modification History tracks changes in sufficient detail to reconstruct the prior versions. If replacement is disallowed, users can save only new versions as separate copies. All of these new versions are tracked in the Modification History. Replacement of signed-off items is not allowed.

Chromeleon facilitates short-term record storage through its built-in backup and restore tools (Figure 8). When a backup of data is created, all relevant raw data, corresponding methods, sequence data, report formats, and audit trails are included.

Long-term storage (archiving) can be provided by creating a Chromeleon archive datasource, which can have read-only restrictions placed on it while remaining fully searchable. Fully traceable, automated backup to this archive datasource can be done using Chromeleon's on-line transfer agent, which performs file operations in environments where users are blocked from direct file access at the operating system level.

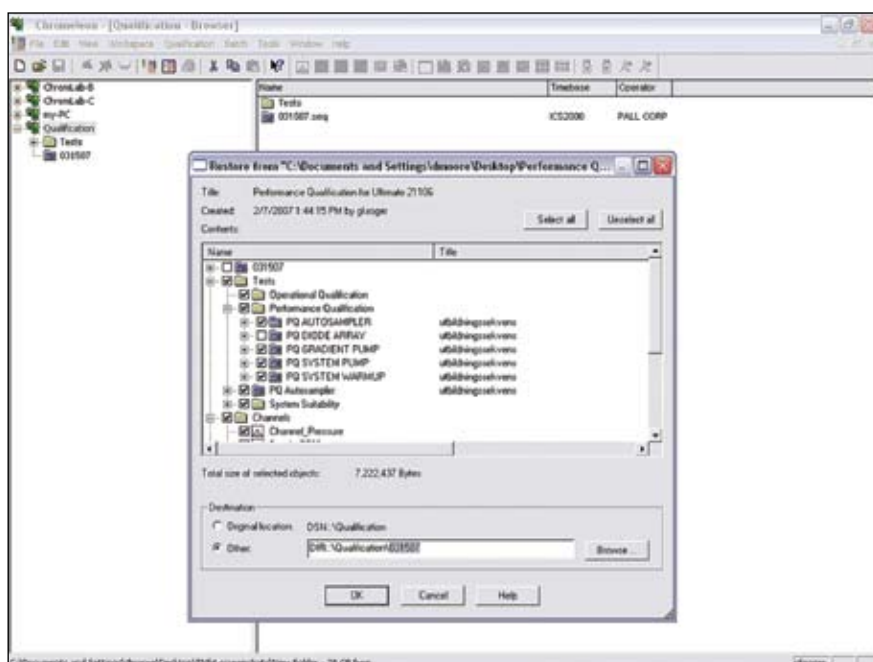


Figure 8. Chromeleon integrated backup and restore utilities facilitate storage of electronic records, while ensuring security and completeness of the records.

**SUBPART B—
ELECTRONIC RECORDS**

**§11.10 Controls for closed systems
(continued)**

- (d) Limiting system access to authorized individuals.

RESTRICTING ACCESS

Chromeleon’s advanced security system supports an unlimited number of security levels and is designed to fit the chromatography workflow.

More than 100 different privileges can be allocated, as appropriate, in any combination and to an unlimited number of different privilege groups (Figure 9). These allow detailed definitions of privilege profiles for different user groups. (For example, Lab Managers would typically be granted privileges to modify integration, whereas Operators might only have privileges to create and run sequences.) Any user can

be granted membership in multiple groups; the resulting privileges are the sum of the privileges provided by the different group memberships.

In addition to Privilege Groups, Chromeleon supports Access Groups. These are used to control access to different instruments and data objects, even for users of the same privilege level. For example, a Lab Manager in Quality Control may have privileges to access and modify analysis data for released products, but can be denied access to data on new compounds being generated by the Discovery group.

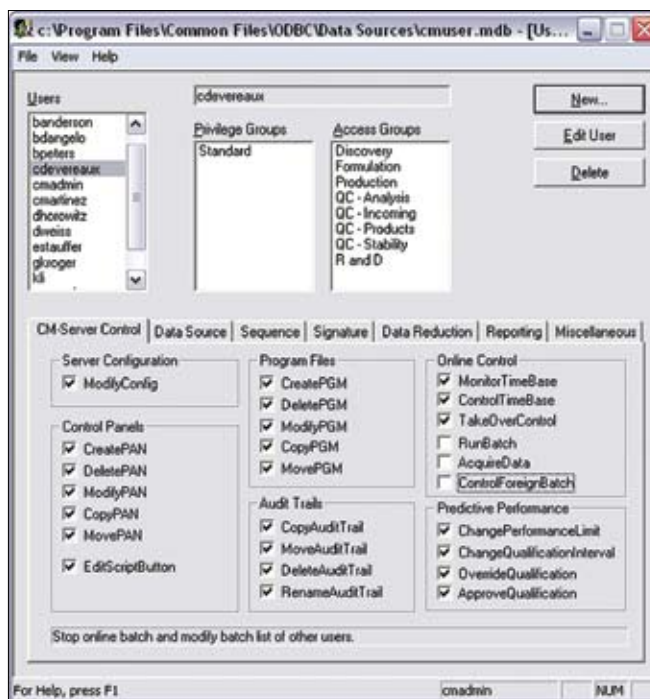


Figure 9. Chromeleon comprehensive, chromatography-specific system gives the System Administrator detailed control over each user’s access to, and privileges for, instruments and data.

Once the Access Groups have been created, access to specific data sources, folders, and/or instruments can be controlled by setting properties for the respective item (Figure 10). Users are allowed to see only the items to which they have been granted access, providing an additional level of security for sensitive data. Folders can also be locked to prevent modification of their contents; privileges for locking and unlocking can be granted separately to different Privilege Groups, as appropriate. Electronically signed records are automatically locked, as discussed in Signature Manifestations Section.

As noted in the Protection of Records section on page 9, Chromeleon users can be completely blocked from direct file operations and access at the operating system level. All user transactions are managed and controlled by the Chromeleon Transaction Agent.

Chromeleon's security system provides the user management capabilities most often requested by system administrators:

- Users are identified by UserID, User Name, and Job Title throughout the software (Figure 11).

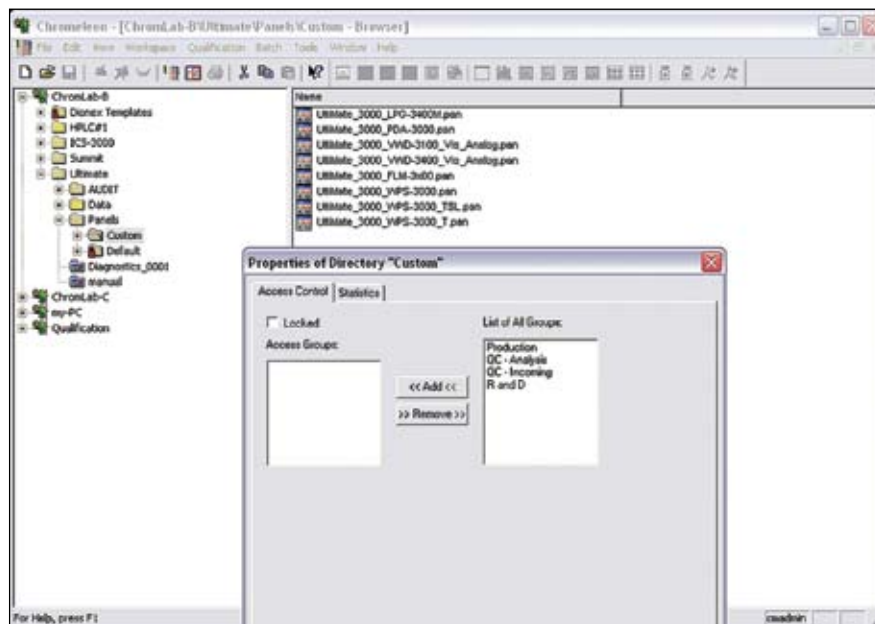


Figure 10. Chromeleon controls access to data sources, individual folders, and instruments. Users who are not members of an access group assigned to an item cannot access or even see the item.



Figure 11. Users are identified by User ID, User Name, and Job Title throughout the software.

- Password controls can be enforced, including minimum password length, password age limits, and password re-use restrictions.
- User and password history logs are maintained automatically (Figure 12).
- Users can be locked out automatically after a pre-set number of login failures (Figure 13).
- Client sessions can be locked automatically after a specified period of inactivity (Figure 14).

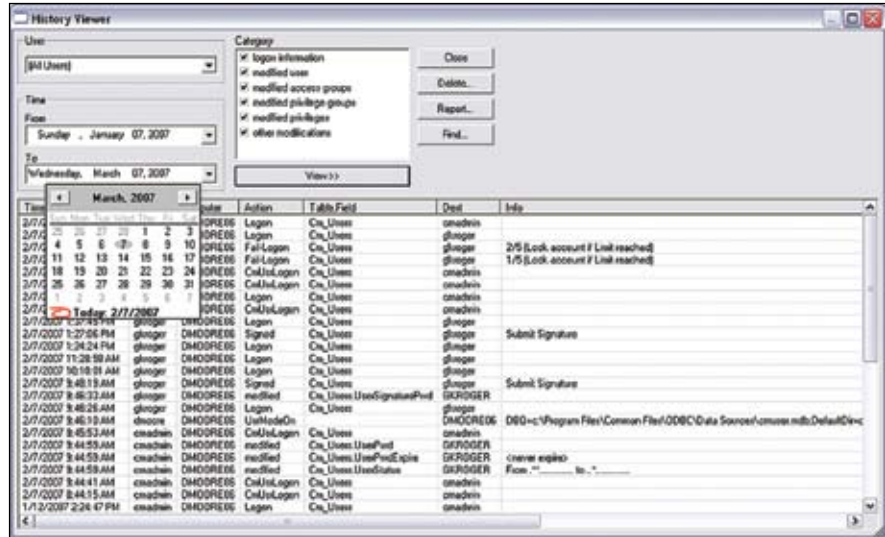


Figure 12. User and password history logs are maintained automatically.



Figure 13. Users can be automatically locked out after a pre-set number of login failures.

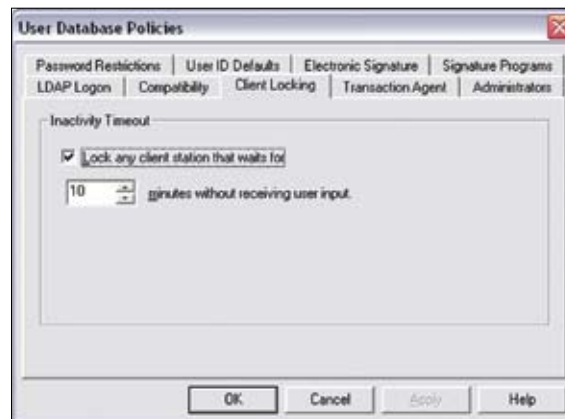


Figure 14. The administrator can set an inactivity timeout policy to help ensure that unauthorized people do not gain access to the system in the event that an authorized user fails to log out before stepping away from a client station.

**SUBPART B—
ELECTRONIC RECORDS**

§11.10 Controls for closed systems

- (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. Record changes shall not obscure previously recorded information. 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.

GENERATION OF AUDIT TRAIL

Chromeleon automatically tracks all operator entries and actions that create, modify, or delete electronic records. It does this by maintaining two types of secure, computer-generated, time-stamped audit trails: System Logs and Modification Histories. Both audit trails record the time and date of each event, along with the identification of the operator involved. Changes to records add new entries to the audit trails, such that previously recorded information is not obscured, and the system administrator has fine control over who is allowed to make changes to data and audit trails.

A daily System Log is created and maintained automatically for each instrument. Each System Log completely documents all events associated with data acquisition and instrument control, including:

- Users connecting to instruments, whether for control or simply to monitor activity
- Sequence starts and stops
- Control commands sent to instruments from an instrument control program or a direct user action
- Responses received from instruments, including any status messages, warnings, or errors
- Instrument configuration changes

Any instrument's daily System Log can be reviewed (Figure 15). List filtering options make it easy to find events of interest. The subset of events pertaining to a particular sequence also can be viewed in real time during instrument operation (Figure 16), or included as a report object (Figure 17).

This detailed documentation not only helps with 21 CFR 11 compliance, it also improves productivity by eliminating the need for manual logging of events and by providing the operators with useful information for tracking their work, and troubleshooting any analysis problems that might occur.

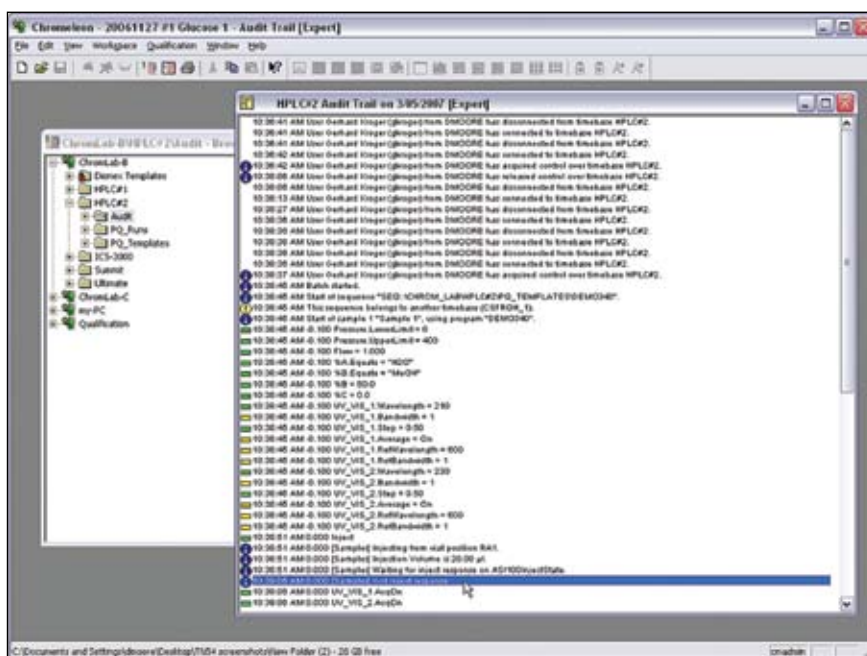


Figure 15. Chromeleon automatically maintains a complete log of each instrument's operator entries and actions that create, modify, or delete electronic records.

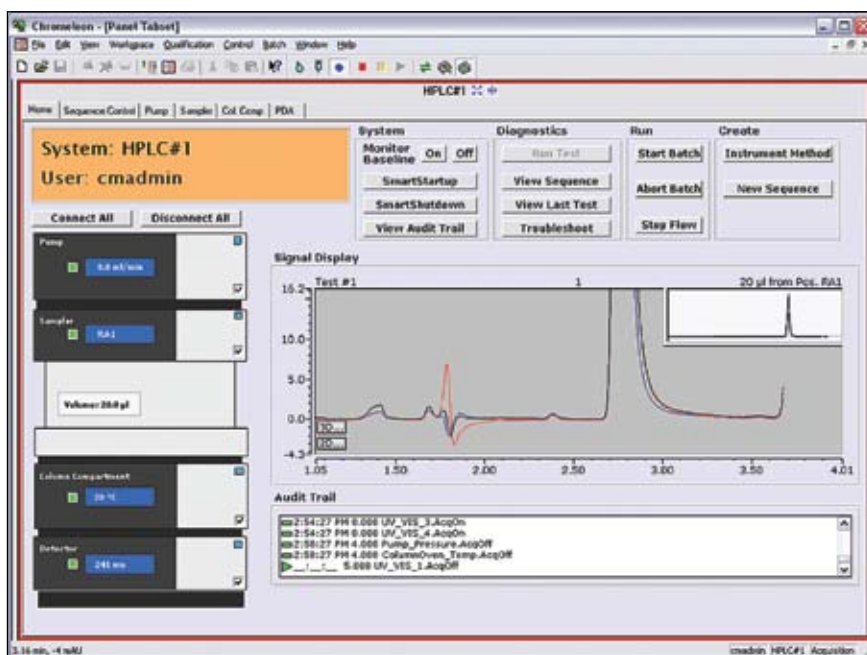


Figure 16. System log events that pertain to the current sequence can be viewed in real time during sample analysis.

The Modification History keeps detailed records of all changes made to data objects and electronic records in a Chromeleon data source. It documents the creation of sequences and related data—including sample entries, instrument control programs, quantification methods and report definitions—as well as all modifications made after the analysis. Post-run modifications include changes to sequence entries, methods and reports; manual baseline adjustments; and any relocation, archival, or deletion of data.

The Chromeleon System Administrator can enable recording of a Modification History for any chromatography data source. By simply right-clicking on an item and selecting {Show History} from the context menu (Figure 18), authorized users can view the history at any desired level of the information hierarchy: individual objects (sample, control program, quantification method, report form, etc.), directory folders, or entire data sources. Users can apply filters to list only events from the current directory, within a current date range, and/or corresponding to a specific operator.

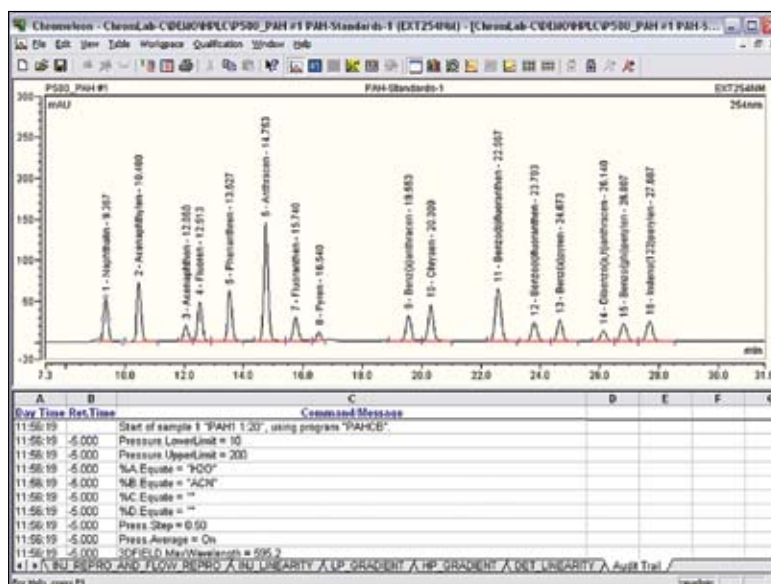


Figure 17. The System Log events for a sequence can be included in the report along with the analytical results, providing full traceability.

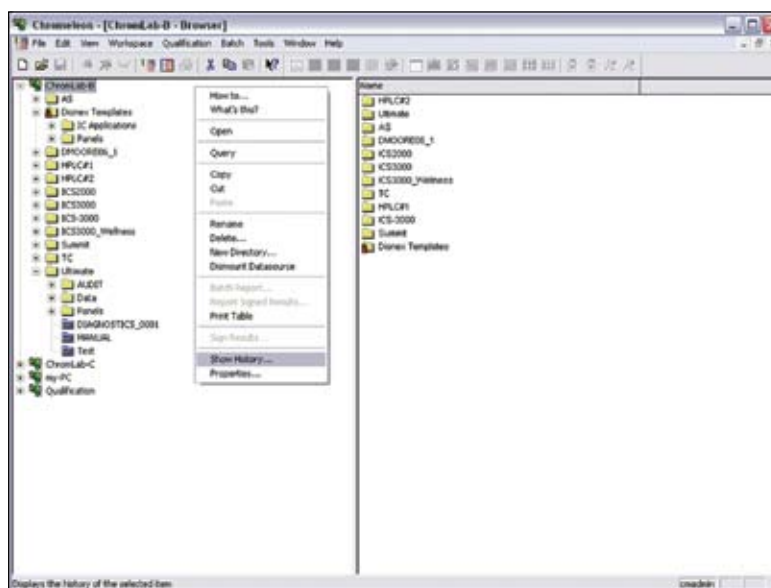


Figure 18. The Modification History of any sample, sequence, folder, or data source can be accessed using the Show History command.

The Modification History display (Figure 19) lists, for each event, the corresponding time and date, affected data object, object version number, operator identification, type of change, and comments. The list can be sorted by any of these fields simply by clicking the corresponding column title. The Details button displays an explicit description of the changes associated with an event, including the prior and current states of the operator entries, detection settings, peak baselines, or any other changed items. The system administrator can allow or require users to enter comments to ensure that intentions are documented clearly.

Chromeleon locks records as soon as they enter the electronic signature process. Locked records cannot be modified by anyone. The System Administrator can restrict who has the privilege to unlock records. Electronically signed records cannot be unlocked unless all signatures are removed. Chromeleon's Modification History tracks all Lock and Unlock operations and all actions in the electronic signature process.

The System Administrator can also prohibit the modification of existing data objects, such that users can save changes only in new versions of the objects.

The binary nature of the audit trail files makes the possibility of falsification remote. However, in an unsecured operating system, it could be possible for a user to gain access at the operating system level and delete or corrupt one of the files cited above. Thus, Dionex recommends that regulated laboratories store all data on secured computers running Windows with the NTFS file system.

Chromeleon provides complete functionality for viewing all audit trails on the system, and for printing hard copies of the audit trails at any time. The hard copies include time/date stamps to facilitate traceability of paper documents.

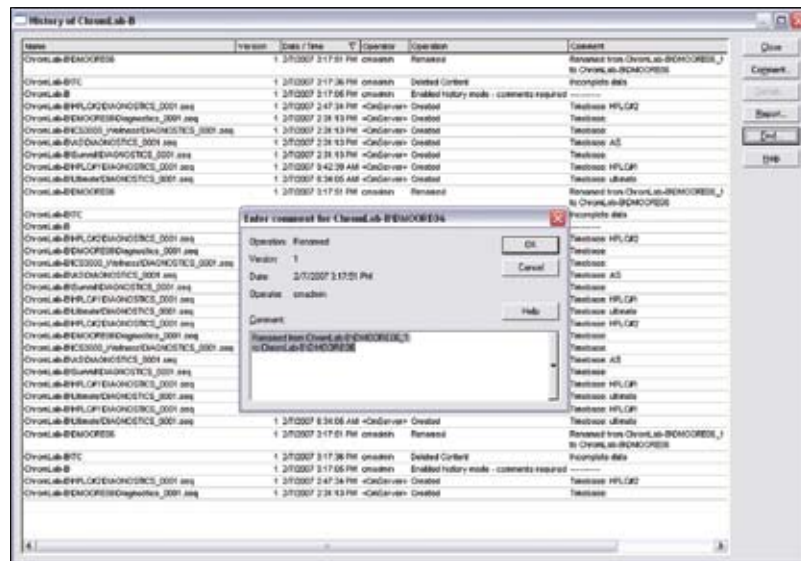


Figure 19. Chromeleon's Modification History tracks all changes to all data objects, and lists the "before" and "after" state of each variable associated with the change.

**SUBPART B—
ELECTRONIC RECORDS**

**§11.10 Controls for closed systems
(continued)**

- (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

**ENFORCEMENT OF CORRECT
STEPS AND EVENTS**

Chromeleon has a context-sensitive structure that hides or disables functions that are not relevant, not appropriate, or not permitted within the current context. This structure helps ensure that steps and events occur in the proper sequence. For example,

if a sequence has been configured to have signature levels of Submitter and Approver, it cannot be approved until it has been signed by a submitter. Chromeleon also provides Wizards (Figures 20 and 21) and many step-by-step procedures with detailed instructions in on-line Help (Figure 22) to further guide users.

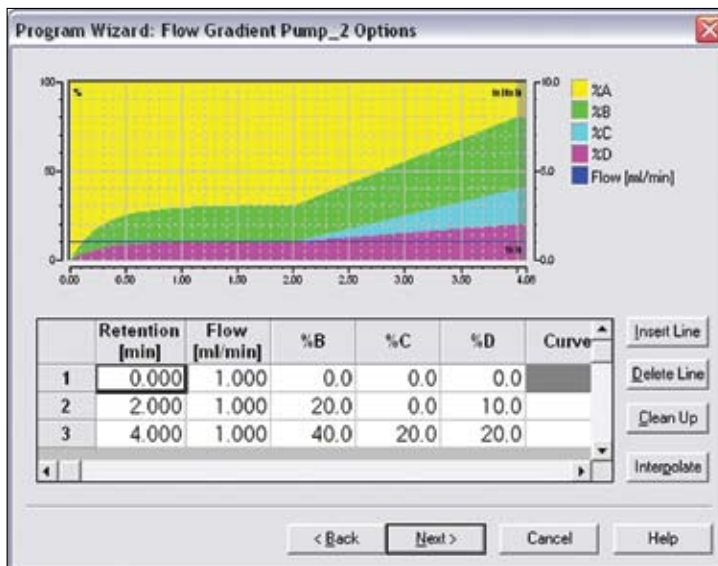


Figure 20. Chromeleon’s Program Wizard guides the user through the steps required to create instrument control programs.

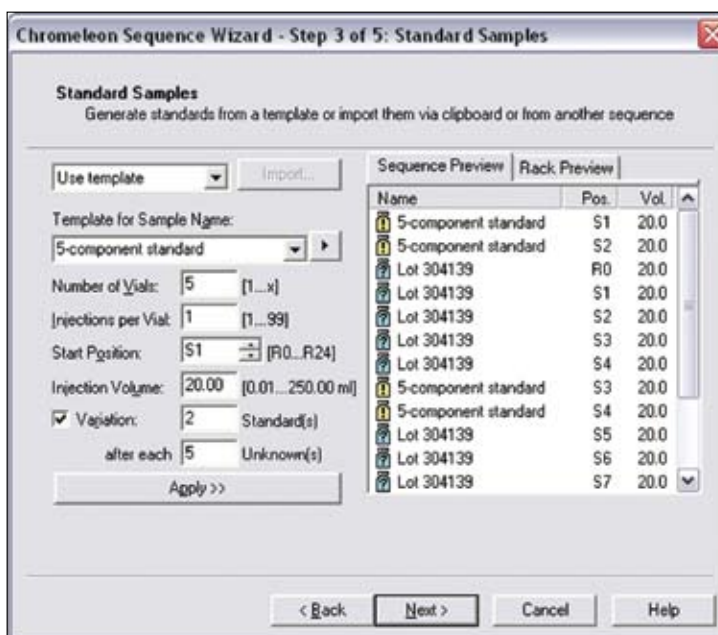


Figure 21. Chromeleon’s Sequence Wizard makes sequence creation fast and easy, and can automatically place standards at regular intervals to comply with SOPs.

Chromeleon performs numerous error checks when instruments are configured, when control programs are defined, and when sequences are readied for execution (Figure 23). Any conflicts must be resolved before the user is allowed to proceed.

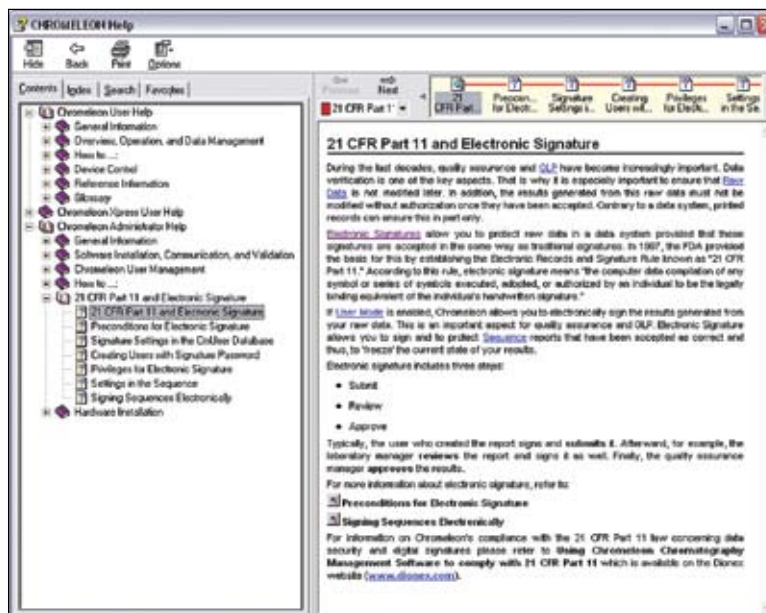


Figure 22. Chromeleon’s on-line Help provides background information as well as step-by-step procedures for all common chromatography operations.

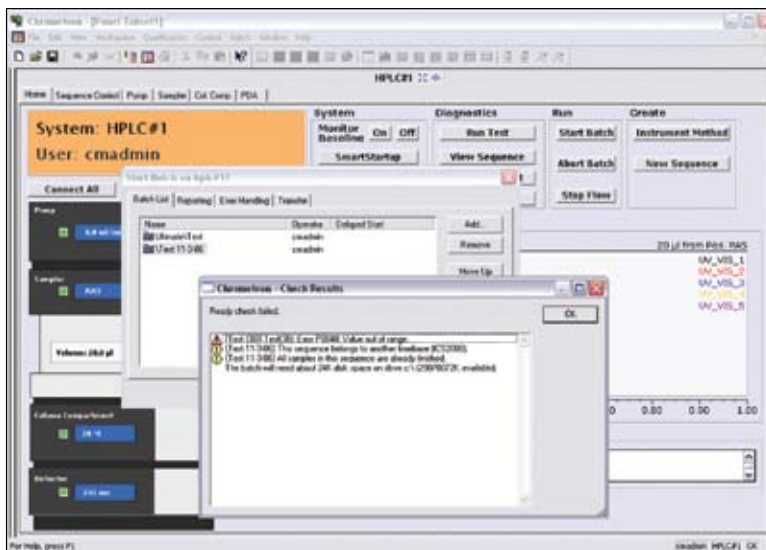


Figure 23. Before executing any sequence or batch of sequences, Chromeleon automatically checks that the instruments are present and functioning, the control programs are valid for the selected instruments, all parameters of the sequence are valid, and sufficient disk space is available for data storage.

**SUBPART B—
ELECTRONIC RECORDS**

**§11.10 Controls for closed systems
(continued)**

- (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.
- (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

AUTHORITY CHECKS

As described under in the Restricting Access section, Chromeleon provides a comprehensive, chromatography-specific security system that controls access to instruments and data, and defines the types of operations that each class of users can perform on the items to which they are granted access. The Signature Manifestations section also details how Chromeleon also controls who is authorized to electronically sign specific sequences.

DEVICE CHECKS

Upon installation, Chromeleon automatically performs a Software Installation Qualification, storing to disk a printable report. Password-controlled logins, both at the operating system level and at the Chromeleon level, to prevent unauthorized access and identify users, regardless of where they log in. Whenever possible, Chromeleon records specific information about the instruments used (serial numbers, operating conditions, vial positions injected, etc.), and checks these against the user-defined configuration. Any differences between the two are flagged.

**SUBPART B—
ELECTRONIC RECORDS**

**§11.10 Controls for closed systems
(continued)**

- (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) 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.

**SUBPART B—
ELECTRONIC RECORDS**

§11.50 Signature manifestations

- (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.
- (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)

**CONTROLS FOR CLOSED SYSTEMS:
EDUCATION AND TRAINING**

Dionex regularly provides appropriate training for its internal developers, service engineers, and support personnel. Records of this training are maintained in accordance with training policies that are registered to ISO 9001.

Dionex provides on-site introductory training for users at the time of installation. Additional training is available and recommended for laboratory managers and for support personnel. System administrators should also attend the Chromeleon Administrator course. Off-site classes are regularly conducted in Dionex field offices. Custom on-site training courses are also available.

**CONTROLS FOR CLOSED SYSTEMS:
DOCUMENTATION OF SYSTEMS**

Dionex supplies user documentation in electronic format on the same read-only media as the software, so that the two are always synchronized. Release notes providing a history of changes from release to release are provided with the software.

MANIFESTATION OF SIGNATURES

Chromeleon's comprehensive implementation of electronic signatures provides all functionality required by 21 CFR Part 11, while also satisfying laboratory workflow needs.

In the Chromeleon security and user management system, the System Administrator can grant specific user groups the privilege of applying electronic signatures (Figure 9). Three privileges—for signing results, for removing signatures, and for modifying sequence signature requirements—allow fine control of user permissions. An individual signature password (separate and distinct from the login password) is also defined for each individual user. Functions such as minimum password length, password uniqueness requirements, password age control, and password history are supported for signature passwords, just as they are for login passwords. For each injection sequence in Chromeleon, persons with appropriate security clearance (the user privilege ModifySignRequirements) can define up to three signoff levels (Submit, Review, and Approve), and either designate specific individuals as signatories, or stipulate that anyone with signature privileges can sign (Figure 24).

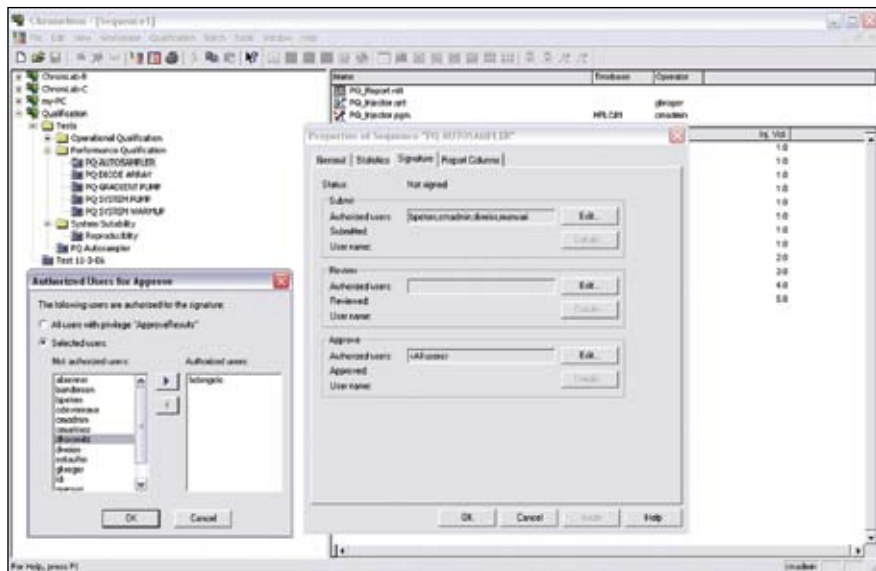


Figure 24. The list of authorized signatories for submission, review, and approval of results can be specified separately for each sequence.

After the correct password is entered, the submission is complete. The sequence remains marked with a special icon indicating that it has been signed (see Figure 25e).

Reviewers and approvers follow the same steps as submitters, but they can review or approve only sequences that have first been signed by a submitter. If a problem is found with the report, an authorized user can undo the signature of the submitter so that necessary modifications can be made; in this case, the report must be resubmitted with a new signature.

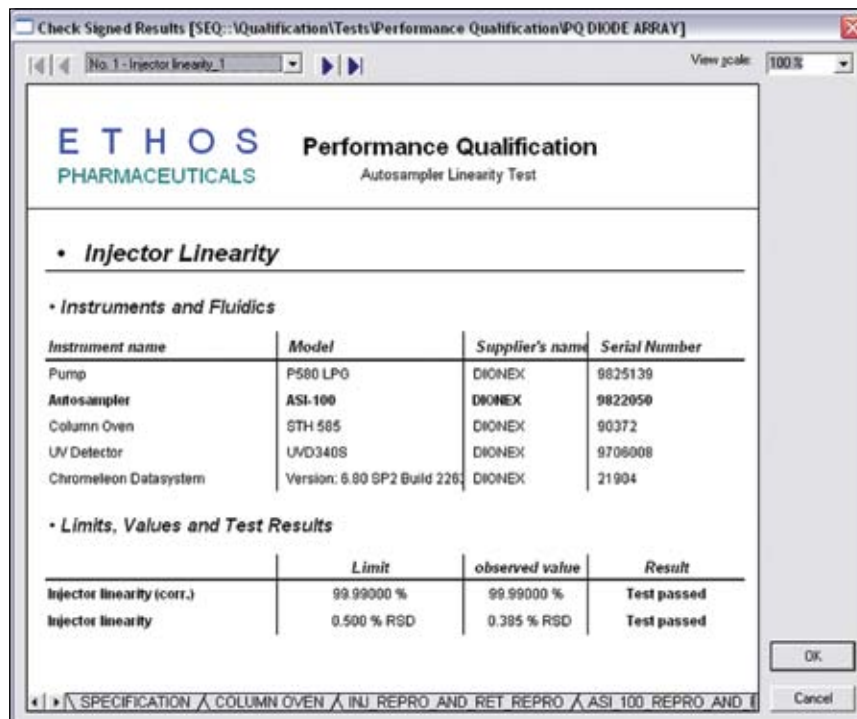


Figure 25d. Before applying the electronic signature to the final report, the user can preview every page to make sure everything is correct.

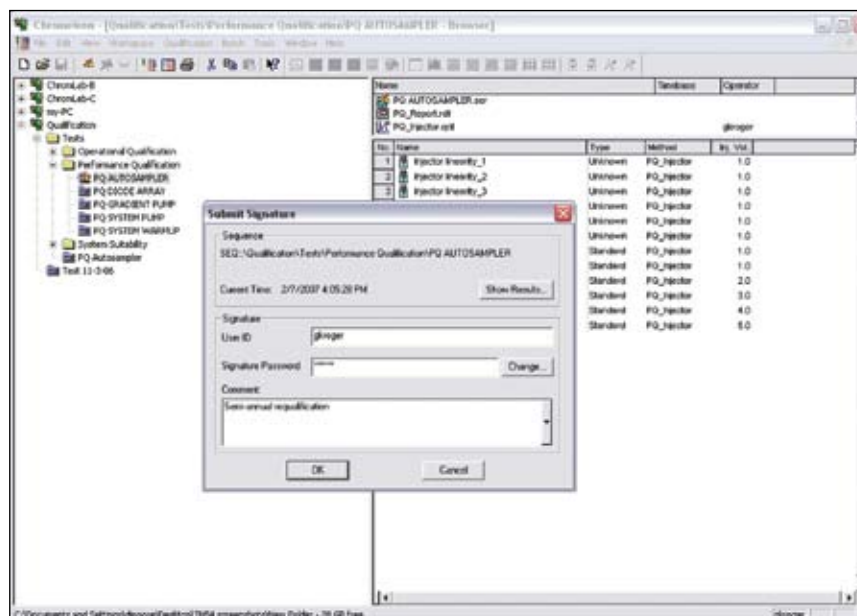


Figure 25e. The user applies the electronic signature to the final report by entering the individual signature password. Using the signature data and the report contents, Chromeleon calculates a hash code that becomes an integral part of the final encrypted report and certifies its authenticity.

Any variables related to electronic signatures (such as signoff status, name of signatory, job title, meaning of the signature, time/date signed, and so forth) can be included in reports (see Figure 2) and used for database queries. Managers can quickly locate all sequences awaiting review or approval by running a simple query (Figure 26).



Figure 26. All sequences awaiting review and/or approval can be rapidly located by running a simple Chromeleon database query.

**SUBPART B—
ELECTRONIC RECORDS**

§11.70 Signature/record linking

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.

SIGNATURE/RECORD LINKING

In Chromeleon, electronic signature data are stored as integral parts of signed-off reports, such that the signature data cannot be excised, copied, or otherwise transferred by ordinary means. When an electronically-signed report is generated, the report contents, user information, and signature time/date stamp are used to calculate a unique hash code; this hash code is stored along with the report contents in an encrypted binary file. If any change is made to the file, the electronic signature is rendered invalid. These security measures make

the possibility of signature or document falsification extremely remote.

Any user can use the Verify command or toolbar button to quickly confirm the integrity of electronically signed documents (Figure 27). The software uses the report data and signoff information to recalculate the unique hash code of the document and confirm that nothing has been altered since the document was created (Figure 28).

Dionex Chromeleon does not support execution of handwritten signatures to electronic records at this time.

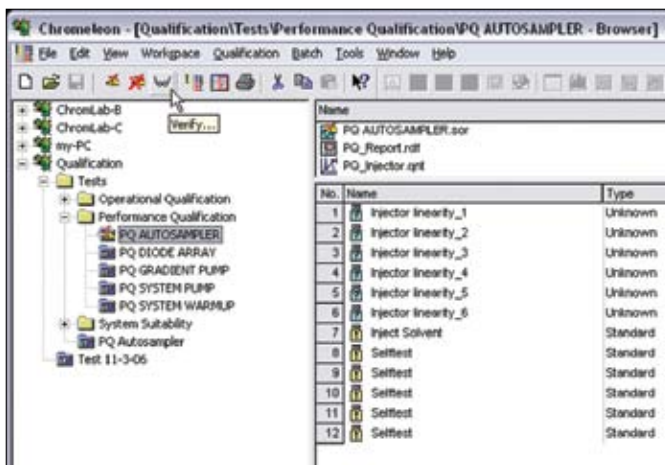


Figure 27. Electronically signed sequences and reports are marked with special icons. Signatures can be checked by selecting the Verify toolbar button or menu command.

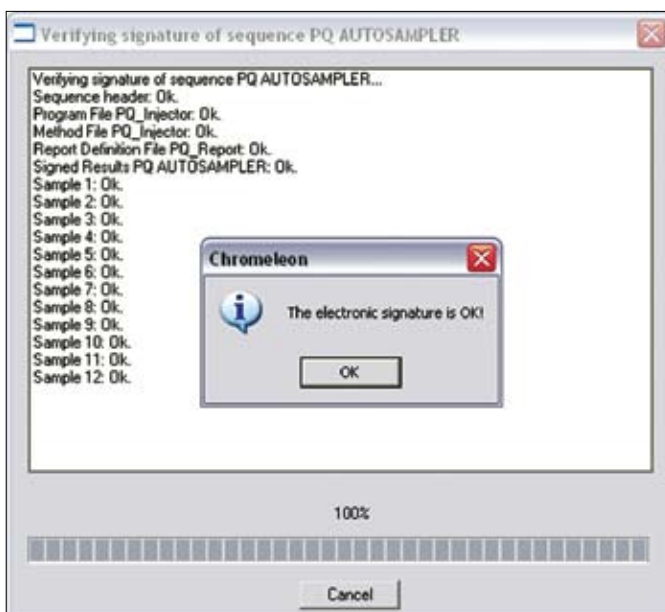


Figure 28. When an electronically signed sequence is verified, the unique hash code is recalculated and compared against the stored value.

SUBPART C—ELECTRONIC SIGNATURES

§11.100 General requirements

- (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.
- (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.
- (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 handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.
 - (2) Persons using electronic signatures 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.

GENERAL SIGNATURE REQUIREMENTS

Chromeleon's electronic signatures are implemented using a combination of a user's unique login name and a signature password. The software requires a unique login name for each individual, so each person's signature combination is unique.

Chromeleon maintains a history of individual login names and signature passwords, and prohibits re-use of each user the 15 most recently used passwords. The System Administrator can require users to change passwords when they next log in, and can set an expiration interval for passwords (Figure 29).



Figure 29. The System Administrator can set password requirements, inactivity timeouts, automatic account disabling, and other policies.

SUBPART C—ELECTRONIC SIGNATURES**§11.200 Electronic signature components and controls.**

- (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.
 - (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.
- (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS

A Chromeleon user must enter their login name and login password to gain access to the system, then enter the signature password each time a sequence is electronically signed. Discontinuity of sessions can be easily enforced through an option that automatically logs a user out if no system activity is detected for a period specified in advance by the System Administrator (see Figure 14).

The login name is unique for each individual, so each person's signature combination is unique and can be used only by its genuine owner. Of course, system users must not reveal their passwords to anyone else; use of the signature by anyone other than the genuine owner would require collaboration of two or more individuals.

SUBPART C—ELECTRONIC SIGNATURES**§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:

- (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 deauthorize 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.

IDENTIFICATION CODES/PASSWORD CONTROLS

Chromeleon facilitates administration of password maintenance through controls such as minimum password length, password age limit, and password re-use prevention. The System Administrator can use these controls to force users to regularly change their passwords to new expressions of a specified minimum length. The System Administrator can also require any user to change a password at next login, and can disable or delete any user account if necessary.

Attempts to breach the security system can be thwarted through automatic account deactivation, which can be set to disable any account after a specified number of failed login attempts (Figure 13).

All security-related events (user and group configuration changes, successful logins, failed logins, and electronic signings) are automatically tracked in Chromeleon's user management data-base. A convenient viewer makes it easy for System Administrators to view particular events of interest; available viewing filters include time/date window, user involved, and event types (Figure 12).

At this time, Chromeleon does not explicitly support use of devices that bear or generate identification codes or passwords.

REFERENCES

1. Federal Register. Vol. 62 No. 54. Thursday March 20 1997. Rules and Regulations. Pages 13429-13466. Available at <http://.fda.gov/ora/compliance/ref/part11/FRs/background/pt11fmr.pdf>
2. 21 CFR Part 11 Guidance Documents. Available at <http://.fda.gov/ora/compliance/ref/part11/FRs/dockets/index.htm>
3. Guidance for Industry - Part 11, Electronic Records; Electronic Signatures - Scope and Application (Issued 8/2003, Posted 9/3/2003). Available at <http://.fda.gov/ora/cder/guidance/5667fml.htm>

Microsoft and Windows NT are registered trademarks and Windows is a trademark of Microsoft Corporation. Oracle is a registered trademark of Oracle Corporation. Chromeleon is a registered trademark of Dionex Corporation.

Passion. Power. Productivity.



Dionex Corporation

1228 Titan Way
P.O. Box 3603
Sunnyvale, CA
94088-3603
(408) 737-0700

North America

U.S. (847) 295-7500
Canada (905) 844-9650

South America

Brazil (55) 11 3731 5140

Europe

Austria (43) 1 616 51 25 Benelux (31) 20 683 9768 (32) 3 353 4294
Denmark (45) 36 36 90 90 France (33) 1 39 30 01 10 Germany (49) 6126 991 0
Ireland (353) 1 644 0064 Italy (39) 02 51 62 1267 Switzerland (41) 62 205 9966
United Kingdom (44) 1276 691722

Asia Pacific

Australia (61) 2 9420 5233 China (852) 2428 3282 India (91) 22 2764 2735
Japan (81) 6 6885 1213 Korea (82) 2 2653 2580 Singapore (65) 6289 1190
Taiwan (886) 2 8751 6655

www.dionex.com



LPN 1302-02 PDF 09/07
©2007 Dionex Corporation