TECHNICAL NOTE

INFRARED SPECTROSCOPY

21 CFR Part 11 Implementation Spectrum ES

Introduction

Compliance with 21 CFR Part 11 is mandatory for pharmaceutical companies and their suppliers to sell products into the United States. Achieving compliance with 21 CFR Part 11 is best accomplished by a partnership between the user and the vendor. The user knows how they want the system to fit into their Quality Management System (QMS) and operate on a day-to-day basis in their organization. The vendor knows how the system achieves compliance within its functionality. The partnership usually consists of the vendor supplying the technical means of becoming compliant and the user adding the procedural means to compliance via working practices, standard operating procedures and fit to their QMS.

The purpose of this document is to allow users and potential users of Spectrum™ Enhanced Security (ES) software to determine how functionality within the software ensures that it meets technical requirements for 21 CFR Part 11 compliance. In addition, areas where standard operating procedures are needed to achieve full compliance are identified. The document is divided into three sections;

- Subpart A, General provisions
- Subpart B, Electronic Records (11.10, 11.30, 11.50 and 11.70)
- Subpart C, Electronic Signatures (11.100, 11.200 and 11.300)

Contents **Page(s)**

Introduction	1-2
System Security	2
Spectrum ES vs. 21 CFR Part 11	2-10
Subpart A – General Provisions	2-4
Subpart B – Electronic Records	4-8
Subpart C – Electronic Signatures	9-10
References	11

PerkinElmer® precisely.

Subpart A is included for background information only and shows the text as detailed in the 21 CFR Part 11 document. Subpart A contains the definitions used in the act.

Subparts B and C contain two columns. The column headed '21 CFR Part 11' includes the text taken directly from the 21 CFR Part 11 document for that section. The column titled 'Spectrum ES' details how the software or the customer meets 21 CFR Part 11 technical requirements.

System security

Spectrum v6 is compatible with Microsoft Windows XP Professional with Service Pack 2 (SP2) only. Spectrum ES utilizes the file security facilities within the Windows XP operating system to increase electronic record security. In addition to the file security, it is recommended that the Windows Administrator secure the appropriate folders using permissions to prevent overwriting and accidental deletion of data.

We also recommend that each user is set-up to use the password-protected screen saver utility within Windows XP, with an appropriate time delay, to protect the system from unauthorized use during a period of inactivity. In addition to Windows XP security, PerkinElmer uses its own security system to control access to the Spectrum ES software, providing a further level of security.

Spectrum ES vs. 21 CFR Part 11

SUBPART A – GENERAL PROVISIONS

	21 CFR Part 11
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.

SUBPART A – GENERAL PROVISIONS

	21 CFR Part 11
11.1 **Scope** *(continued)*	
11.1 (f)	This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.
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, 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 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.
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.

SUBPART A – GENERAL PROVISIONS

	21 CFR Part 11
11.3 **Definitions** *(continued)*	
11.3 (b) *(continued)*	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.

SUBPART B - ELECTRONIC RECORDS

	21 CFR Part 11	Spectrum ES
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.	It is the customer's responsibility to develop appropriate validation protocols for the system, however, PerkinElmer provides tools and services to assist in the DQ, IQ, OQ and PQ of the system. Within Spectrum ES, software is provided to enable the automatic verification of instrument performance. Reference materials and recalibration services are available from PerkinElmer. To ensure that only operators trained to use the system can access the system, Spectrum ES uses an admission system requiring a User ID and password. Data includes a checksum to ensure provenance and prevent tampering. Spectrum ES will reject data with an invalid checksum.
11.10 (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 a review and copying of the electronic records.	On screen viewing of spectra, results, reports and audit trails are possible. Spectrum ES also has printing and export utilities to facilitate this.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	When spectral data is generated individually, they can be immediately and automatically saved. If a sample table of data are being generated when a power failure occurs, data sets are recovered when restarting the software and attempting to scan new data. The customer must provide guidelines to operators for changes to other types of data.

SUBPART B – ELECTRONIC RECORDS

	21 CFR Part 11	Spectrum ES
11.10 **Controls for closed systems**		
11.10 (c)	*(continued)*	Spectrum ES consists of electronic data (user names and passwords) contained within a database and as individual files (spectra, peak tables, etc) in the Windows file structure. It is the customer's responsibility to introduce a suitable backup procedure for electronic data records. The Spectrum ES Administrator's guide provides guidelines to assist in this procedure. We recommend that archived data are protected to prevent loss in the event of a total or partial loss due to a catastrophic failure, for example fire.
11.10 (d)	Limiting system access to authorized individuals.	A unique user name and secret password is required for all authorized users. Two password login modes are available, PerkinElmer Login and Windows Login. With PerkinElmer login, the logins (username and password) remain unique within the system even after a user has left the company. Passwords cannot be viewed by anyone, including the system administrators or PerkinElmer. With Windows login, the login and login security settings are controlled by the login to the Windows operating system. All access or attempted access to the system is logged. Regular review of the log is customer/client responsibility, and should be part of the system's procedural compliance. Users are limited to a number of unsuccessful login attempts (i.e. wrong password). If the set number of unsuccessful logins is reached, that user name is suspended. A system administrator will be notified that a user name has been suspended the next time that they start the software. A Spectrum ES administrator can allocate a new temporary password, which the user is forced to change on its first-time use (i.e. their next login). Due to the high degree of security in Spectrum ES, it is highly recommended that more than one administrator be created in case the administrator is absent or forgets their password. The product has no 'back-door' to the security system.

SUBPART B – ELECTRONIC RECORDS

	21 CFR Part 11	Spectrum ES
11.10 **Controls for closed systems** *(continued)*		
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. 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.	A spectral audit trail (spectrum history) is available as part of the status of the spectrum. This records all actions applied to the spectrum, and by whom, that affect the data. These actions are typically of a processing nature (Abs., interpolation, etc.) The security audit trail history contains the user name of the user, the full user name, the date and time stamp when the record was created, modified or deleted, the new value, the old value and the type of modification (e.g. insert, delete, modify etc.). Changes to records do not obscure previous entries. Audit trails can be viewed, printed and exported for inspection purposes.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Spectrum ES has several mechanisms to allow enforced sequencing: • Individual roles are enforced through the assigning of individuals to Groups: Administrator, Supervisor and Analyst, are examples of typical groups. The groups to which a user belongs defines the areas of the software he or she is permitted access to. • 'Learn mode' procedures can be developed to automate data processing. It is the responsibility of the customer to develop these procedures. • The system performs checks to ensure data collected is valid. For example, changing accessory or changing to a higher spectral resolution will enforce a new background collection.
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.	Spectrum ES enforces authority checks through the use of authorization groups. Each group has its software access rights defined by the selection of the menus and toolbars that group will be able to access. At installation, Spectrum ES has a default set of authorization groups. A Spectrum ES administrator can alter the permissions of these groups and add new groups to the system. This allows the application to be customized to their way of working. Members of the Administration group may access administration tasks, maintain the system and allocates areas of access to individual users.

SUBPART B – ELECTRONIC RECORDS

	21 CFR Part 11	Spectrum ES
11.10 **Controls for closed systems** *(continued)*		
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.	Spectrum ES will only read recognized 21 CFR encrypted PerkinElmer file formats. More than one instrument may be added to Spectrum ES. During installation, the instrument model and serial number are checked for validity. Instrument model and serial number are stored with all data collected. Data is protected by a checksum. Spectrum ES will produce an error should this checksum become invalidated either by accidental or intentional modification.
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 service engineers are trained and are certified in order to install service and maintain PerkinElmer FT-IR Spectrometers. End user training is the responsibility of the client and should be part of the system's procedural compliance. PerkinElmer provides a series of multimedia tutorials on the spectrometer and accessories together with a set of software tutorials. All tutorials finish with a series of questions that must be answered to provide certification of the user. Electronic (help files) and hardcopy documentation is also provided to assist in developing customer specific training material. PerkinElmer can also provide in-house or off-site training on the spectrometer and/or software to assist in this requirement.
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.	It is the responsibility of customer and should be part of the system's procedural compliance.
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.	It is the responsibility of customer to maintain appropriate controls of the installed system and should be part of the system's procedural compliance. PerkinElmer follows a structured development procedure called PACE (Product And Cycle time Excellence). Details of this process are available on request. Written procedures control the development, testing and maintenance of the systems. Procedures have appropriate approval signatures; and an established, documented method for the creation, review and approval.

SUBPART B – ELECTRONIC RECORDS *(continued)*

	21 CFR Part 11	Spectrum ES
11.30 **Controls for open systems**		
	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.	**NOT APPLICABLE – Closed system only**
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.	Spectrum ES does not have signed electronic records.
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).	Spectrum ES does not have signed electronic records.
11.70 **Signature/recording 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.	Spectrum ES does not have signed electronic records.

SUBPART C – ELECTRONIC SIGNATURES

	21 CFR Part 11	Spectrum ES
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.	Spectrum ES does not have signed electronic records.
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.	Spectrum ES does not have signed electronic records.
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.	Spectrum ES does not have signed electronic records.
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.	Spectrum ES does not have signed electronic records.

SUBPART C – ELECTRONIC SIGNATURES

	21 CFR Part 11	Spectrum ES
11.200 **Electronic signature components and controls**		
11.200 (a) *(continued)*	(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.	
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.	Spectrum ES does not have signed electronic records.
11.300 **Controls for identification codes/passwords**		
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.	Spectrum ES does not have signed electronic records.
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).	Spectrum ES does not have signed electronic records.
11.300 (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.	NOT APPLICABLE
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.	Spectrum ES does not have signed electronic records.
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.	NOT APPLICABLE

References

1. Title 21 of the Code of Federal Regulations, Part 11 – "Electronic Records; Electronic Signatures." Released on 20th March 1997 and became effective on 20th August 1997. Revised 1st April 2005.

PerkinElmer Life and Analytical Sciences
710 Bridgeport Avenue
Shelton, CT 06484-4794 USA
Phone: (800) 762-4000 or
(+1) 203-925-4602
www.perkinelmer.com

PerkinElmer®
precisely.

For a complete listing of our global offices, visit www.perkinelmer.com/lasoffices

007536_01