

## Statement of Software Compliance with 21 CFR Part 11

***Applicable Products: Eksigent NanoLC Software for Express-100 and Express-800 HPLC systems. Current as of 4/22/04.***

Eksigent is committed to providing software tools for its customers that facilitate their compliance with U.S. FDA regulations. Eksigent's instrument control software provides its customers with a robust, reliable platform that continues to evolve to meet their changing requirements. In support of this commitment, Eksigent intends to provide software that helps its customers meet the requirements of the FDA Electronic Records and Electronic Signatures Rule (21 CFR Part 11).

The following is a summary of the 21 CFR Part 11 requirements (subpart B – Electronic Records) as they apply to the Eksigent NanoLC software, the approaches taken to comply with the requirements, and current implementation status.

Addressed requirements:

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

Eksigent provides validation services as part of its installation and qualification of the instrument. All electronic records generated by the Eksigent software, including electronic signatures, chromatographic data, system, and method information are verified prior to their use within the software as described in the following sections.

*Current status: These requirements are met for the functions included in the current software release (2.04).*

### **§ 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.**

The ability to view, print, and export the content of electronic records, such as audit trails, system settings, chromatographic information, etc. to other portable document formats such as Excel, PDF, or text files is included to allow complete and accurate paper and electronic copies for FDA submissions.

*Current status: These features are implemented in the current software release (2.04).*

**§ 11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.**

Each record entry is stored and validated with a unique 128-bit "fingerprint" (RSA Data Security, Inc. MD5 Message-Digest Algorithm) to authenticate retrieved records. This authentication can detect attempts of external tampering and ensures that even those users who have access to files at the operating system level cannot modify records through means outside the secured application. In addition, data corruptions due to defects or failure of storage devices or media, or deliberate attempts to modify records are also detected and reported by the software.

*Current status: These features are implemented in the current software release (2.04).*

**§ 11.10(d) Limiting system access to authorized individuals.**

The system has multiple levels of security. Each user is assigned an account with a unique username and password, both of which are required to log on to the system. The user's identity and role, which can be assigned by project, are combined with the access control system attributes to determine whether access to a procedure should be permitted or denied.

*Current status: These features are not included in the current software release (2.04). Compliance with this requirement is scheduled for the September 2004 software release.*

**§ 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.**

Audit trail records (logs) of all system parameters and tasks are recorded in proprietary protected log files. This log is a secure record of all attempts to access or log onto the system together with the operations performed. All records are computer generated and time-stamped to facilitate traceability. The contents of the log files include the person making any change, a time-stamp, and both the original and changed data. The audit trail logs are periodically archived and evidence of previously changed or deleted data is easily accessible and visible. These audit trail records are periodically archived, and are available to be viewed within the program, printed, or exported to other electronic

document formats. The validity of each audit trail record entry, including time-stamps, is ensured with the record protection method described in 11.10(c).

*Current status: These features are implemented in the current software release (2.04), with the exception of auditing of attempts to access or log onto the system. This feature is scheduled for the September 2004 software release.*

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

The software 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. The software performs numerous error checks when instruments are configured, calibrated, and when sequences are readied for execution. Any conflicts or invalid non-verifiable settings are clearly indicated to the user and must be resolved before the user is allowed to proceed.

*Current status: These features are implemented in the current software release (2.04).*

**§ 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.**

The Eksigent software uses a combination of a username and password to authorize an electronic signature. Access to the software is governed by an internal secure database, which defines individual user permissions. All users are required to log on using Windows authentication and password procedures, which enforce password aging, length/format, uniqueness, and lockout.

*Current status: This feature is not included in the current software release (2.04). Compliance with this requirement is scheduled for the September 2004 software release.*

**§ 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.**

Upon installation, the Eksigent software automatically verifies that all software components are correctly installed. A report is stored to disk and can be printed. The software also records specific information about the actual instruments used (firmware versions, device serial numbers, etc.).

*Current status: These features are implemented in the current software release (2.04).*

**§ 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.**

Eksigent regularly provides appropriate training for its developers, service engineers, and support personnel. Records of training are maintained in accordance with training policies that are documented in Eksigent's Analytical Instrument Quality Manual.

Eksigent provides on-site introductory training for users at the time of installation. Additional training is recommended for system administrators, laboratory managers, and other support personnel. Custom user on-site training is also available.

*Current status: These procedures are implemented in the current software release (2.04).*

**§ 11.10 (j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated their electronic signatures, in order to deter record and signature falsification.**

Eksigent customers are responsible for establishing and enforcing procedures that support the use of the Eksigent software in any regulated environment.

**§ 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 modification of systems documentation.**

Eksigent provides CD-ROM and hard copy manuals for all its products. Release notes providing a history of changes from release to release are provided with the software. The software version covered by the manual is identified in the front of each manual. These manuals are normally part of the initial system delivery. Customers are responsible for ensuring proper control of release levels and distribution of manuals supporting the products, and any internal application documentation.

*Current status: These processes are implemented in the current software release (2.04).*

**§ 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.**

Eksigent customers are responsible for the development of procedures and controls associated with the use of manufacturing applications in any regulated situation.

**§ 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 are executed by the user through the software user-interface, where the user is required to enter her username and password (see 11.200). The electronic signature is stored in the database along with the name of the unique identifier of the document, the signer's full name, the date and time the signature was executed, and the meaning of the signature. Functions such as minimum password length, password uniqueness requirements, password age control, and password history are supported. When viewing or printing the record from within the system, a signature page is displayed / printed which will include all required items.

*Current status: These features are not included in the current software release (2.04). Compliance with this requirement is scheduled for the September 2004 software release.*

**§ 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.**

From within the system it is impossible to remove, modify, or transfer an existing electronic signature. An electronic signature is linked to each specific electronic

record. Electronic signature information is stored as a required component of relevant records, such as reports, methods, chromatographic data, etc. All information is under the same controls as any other record in the system (11.10c) including tracking of modifications and audit trail, and therefore the signature cannot be excised, copied, or transferred using ordinary means.

*Current status: This requirement is not included in the current software release (2.04). Compliance with this requirement is scheduled for the September 2004 software release.*

**§ 11.100(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.**

Each username/password combination is unique. User accounts can be disabled by an administrator but cannot be removed from the system, thus the system enforces that the signature cannot be reused or reassigned.

*Current status: This requirement is not included in the current software release (2.04). Compliance with this requirement is scheduled for the September 2004 software release.*

- § 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.**
  - (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.**

Electronic signatures are implemented using a username and password combination to authorize a signature. The user must enter the login name and login password to gain access to the system, and then enter the signature password each time a sequence is electronically signed. Continuity of sessions is maintained by logging out a user if no system activity is detected for a period whose length is specified in advance by the system administrator. Each user's username and password is unique, and should only be known by its genuine

owner, thus attempted use of the signature by anyone other than the genuine owner would require collaboration of two or more individuals.

*Current status: These features are not included in the current software release (2.04). Compliance with this requirement is scheduled for the September 2004 software release.*

**§ 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.**

The Eksigent software does not use biometric authentication techniques. Instead, a user of the system enters her username and password combination to authorize a signature.

**§ 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:**

**§ 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.**

The Eksigent software enforces the requirement that each combination user id / password is unique.

*Current status: This feature is not included in the current software release (2.04). Compliance with this requirement is scheduled for the September 2004 software release.*

**§ 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).**

The Eksigent software allows for passwords to expire after a set period of time.

*Current status: This feature is not included in the current software release (2.04). Compliance with this requirement is scheduled for the September 2004 software release.*

## References

***21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule  
Electronic Submissions;***

Department of Health and Human Services

Food and Drug Administration

Establishment of Public Docket; Notice

March 20, 1997

[Docket No. 92N-0251]

RIN 0910-AA29

***Guidance for Industry Part 11, Electronic Records; Electronic Signatures —  
Scope and Application***

Division of Drug Information, HFD-240

Center for Drug Evaluation and Research (CDER)

**August 2003**

*Pharmaceutical cGMPs*