



# Factrol 3.1

## CFR 21 Part 11 Compliance Overview

Page 1 of 10

07/25/2003

### ***Annotated Rule***

The following complete text CFR 21 Part 11 has been annotated, when appropriate, to indicate the means used by Factrol control systems to conform to the guidelines established by this rule. Where no annotation is provided for a section, the authors considered such annotation to be unnecessary due to the topical nature of that section. Factrol systems contain numerous features and safe guards intended to comply with this rule. However, compliance cannot be achieved unless certain necessary steps are also taken by the customer. When such steps are indicated, annotations have been added to the rule below.

Fluid Air, Inc. endeavors to remain current with regulatory and industry interpretation of this and other GMP rules. As such, Fluid Air will make amendments to this compliance strategy, when deemed necessary by the company, to maintain compliance with CFR 21 Part 11 as it is presently understood and enforced.

### **TITLE 21--FOOD AND DRUGS**

### **CHAPTER I--FOOD AND DRUG ADMINISTRATION, DEPARTMENT OF HEALTH AND HUMAN SERVICES**

### **PART 11--ELECTRONIC RECORDS; ELECTRONIC SIGNATURES--Table of Contents**

#### **Subpart A--General Provisions**

#### **Sec. 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.



## Factrol 3.1

### CFR 21 Part 11 Compliance Overview

Page 2 of 10

07/25/2003

- (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 Sec. 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.

#### **Sec. 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.



## Factrol 3.1 CFR 21 Part 11 Compliance Overview

### Sec. 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.

*Factrol control systems, installed so that direct access to the system hardware and interface are limited to authorized personnel only, are considered closed systems. Limiting access to the interface and hardware are the determining criteria for establishing a system as closed. The responsibility to implement and enforce the necessary security controls rests with the customer.*

- (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.



## Factrol 3.1

### CFR 21 Part 11 Compliance Overview

Page 4 of 10

07/25/2003

- (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

##### Sec. 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.

*Fluid Air provides complete control system design and test documentation with every system. Additional I/Q and O/Q services are available.*

- (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.

*Factrol provides for viewing and printing of batch data and product recipes. Batch data can be exported in non-native formats (such as comma-delimited).*

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

*Factrol provides means for the archiving and retrieval of batch records. Additional means are provided for backing up electronic records to network or removable media drives. The customer is responsible for implementing an appropriate data backup procedure.*

2550 White Oak Circle Aurora Illinois 60504-9678  
Phone-630-851-1200 Fax-630-851-1244



## Factrol 3.1 CFR 21 Part 11 Compliance Overview

Page 5 of 10

07/25/2003

- (d) Limiting system access to authorized individuals.

*Factrol provides a robust security system including optional radio proximity badge readers. Together with user generated and maintained security procedures, access to the system is limited to authorized individuals.*

- (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.

*Factrol maintains several audit trails to capture user activities relating to electronic records. In some cases these audit trails also capture actions that are outside the scope of this document. Factrol's audit trails include:*

- a) *Batch Data Audit Trail: This log captures data log (record) start and stop commands, archiving, exporting, and operator actions that have the potential to impact the batch.*
- b) *Calibration Audit Trail: This log captures calibration events and any modifications to sensor information.*
- c) *Recipe Audit Trail: This log captures the revision history of recipes.*
- d) *Password Security Audit Trail: This log captures every log-on attempt, successful or otherwise, electronic signature attempt, successful or otherwise, user and group status, permission changes, and every log-off.*
- e) *Independent Database Log Files: Each database is documented by a separate and fully independent log file. This file details every transaction with the database. Processing this file can recreate the database. Altering this audit trail renders the database inoperable.*

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

*Factrol can enforce sequencing for batch record creation and for certain signing (required user input) events. Factrol automates the collection of data at regular intervals or upon event occurrence. Order of operation is not important for other operations concerning electronic records. Phases enforce order of operation for batch processing.*



## Factrol 3.1 CFR 21 Part 11 Compliance Overview

Page 6 of 10

07/25/2003

- (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.

*Factrol provides a robust security system including optional radio proximity badge readers. Together with user generated and maintained security procedures, access to the system is limited to authorized individuals.*

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

*Factrol control systems are designed as single user systems with one user interface location. Terminal checks are not appropriate for this architecture.*

- (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.

*Fluid Air provides and documents the training required by our in-house and field engineering staff. Training for system users is the responsibility of the customer.*

- (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.

*This is the responsibility of the customer.*

- (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.

*Fluid Air provides electronic copies of User Manuals and Validation Manuals. The customer is responsible for implementing the appropriate controls for this documentation.*



## Factrol 3.1 CFR 21 Part 11 Compliance Overview

Page 7 of 10

07/25/2003

- (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

*Fluid Air maintains change and version control for all Factrol User Manuals. The customer is responsible for implementing appropriate controls for this documentation once control of the document is transferred from Fluid Air.*

### **Sec. 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 Sec. 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.

### **Sec. 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.

*User Confirmations include the name of the signer, time/date confirmation was given, meaning of the requested confirmation, and any additional commentary concerning the confirmation that the user felt it was germane to include.*

- (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).

*Reports can be generated that include only signature information that was applied to a batch record. All data and message batch record printouts, as well as recipe printouts, contain the name of the signer(s), the applied time/date of the signature(s), the signature meaning(s), and user commentary(s).*



# Factrol 3.1

## CFR 21 Part 11 Compliance Overview

### Sec. 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.

*Confirmations can only be applied to the record by the control system. No access is granted to the data records through ordinary means.*

### Subpart C--Electronic Signatures

#### Sec. 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.

*Once a User Identification is assigned, it cannot be reused or reassigned on Factrol control systems. User Identifications can be de-authorized.*

- (b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

*This is the responsibility of the customer.*

- (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.

*Compliance with this section is the responsibility of the customer.*



## Factrol 3.1 CFR 21 Part 11 Compliance Overview

### Sec. 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.

*Factrol employs a discrete public user identification and a private 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.

*Factrol does not make use of this exception. Factrol always requires both signature components to be used for any signing.*

- (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.

*Factrol's security system meets this requirement. The customer will also need to implement appropriate procedures so as not to violate this rule.*

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

*Currently, Factrol does not use biometric ID's.*

### Sec. 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:



## Factrol 3.1 CFR 21 Part 11 Compliance Overview

Page 10 of 10

07/25/2003

- (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.

*Factrol does not allow the reuse of user identifications. As such, all user identification – password combinations are unique.*

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

*Factrol enforces 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.

*Factrol allows the de-authorization of user identifications and/or radio proximity badges. Factrol allows passwords to be changed if compromised. The customer is responsible for implementing the necessary security S.O.P.'s to cover these events.*

- (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.

*Factrol will de-authorize any account against which three successive failed logon attempts are made. When a locked out user successfully enters the correct user identification and password combination, the user is notified of the locking but no permissions are given. When a non-locked user successfully logs on when a user is locked, notification is given that a user is locked. A user with permission to edit user and group permissions has authority to unlock users who are locked. Factrol logs locking and unlocking events to the Password Security Audit Trail. The customer is responsible for implementing the necessary S.O.P.'s to cover these events.*

- (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.

*Factrol provides for the testing of radio proximity badges. The customer is responsible for implementing an appropriate periodic testing regimen.*