RoeLee and 21 CFR Part 11

J.S. Fry

2nd May 2003

Introduction

RoeLee software for recording and analysing data, with special provision for necropsy and histopathology, has been in use since 1984. It has always concerned itself with security and after discussion with users brought in the concepts of signing off animals and keeping audit trails. The specification for this is given in Appendix I.

The basic idea of the original RoeLee specification was to have a simple continuation of the current practice when using paper systems. In a paper system, when the pathologist was satisfied that the correct information had been entered into reports for all the animals, he/she would print out the reports and then check, sign and date the paper copies. These paper copies would then be the actual raw data for an experiment. In RoeLee we introduced the idea of ratification, so that when the pathologist was satisfied with the electronic form of information he would ratify the animal, by first validating the animal (that is ensuring that data had been entered for all the relevant organs and findings) then checking the electronic report on the animal and finally signing off the animal. From that time any changes to the animals would be noted on an audit trail, requiring the pathologist to given a reason for the change.

Entering histopathology data is essentially a one person affair. There is a degree of subjectivity which means that when judging severity of lesions it is difficult for even one pathologist to keep consistent. Thus, it was always imagined that there would be one main user who would be the only person to be able to enter data on the system, while other users would be given lesser permissions which would allow them to report and analyse the data. It seemed to us that as long as the environment the pathologist was working in had fairly strong security to stop non-authorised people from accessing the electronic files, the pathologist, and hence the FDA, could be confident that the data reported were the data they had entered and signed off. Indeed for single pathologists working at home and for pathologists working within VAX/ALPHA systems we feel confident that the system works well.

In the last few years the FDA has become more concerned about the changeover from paper to electronic records and have worked to codify situations in which they would feel satisfied that the electronic records are secured and that they could be confident that the results that they are presented with accurately reflect the findings of a named, registered pathologist. This work has led to an amendment to Chapter I of the Code of Federal Regulations by adding a part 11 which concerns itself with Electronic Records and Electronic Signatures. This amendment is given in Appendix II – it is only a few pages long, but the amount of "explanatory" information that is in the public domain is too vast even to summarise. In RoeLee we have adopted the approach that we believe that the FDA require good science to be done and to be seen to be done. That means that we

must be able to verify who has done what and when, and in particular, that the results seen by the pathologist are what is presented to the FDA. In our reading of the Part 11 this is what the FDA is concerned with. Other people who wish to further their own interests by adding complexity to systems which are outside the scope of both Part 11 and the science involved should be discouraged.

At RoeLee we have examined in detail the Part 11 amendment and decided to enhance the RoeLee system to add features we feel necessary to fulfil the requirements as specified. We are proposing the following changes:

1. Usernames and Passwords

In the current version of RoeLee (2.05), PC users only need enter an 8 character password to enter the system. The username is set-up on initialisation and is not usually shown to the user. Current practice elsewhere is to show usernames and then require a password for a given username. Thus in the next version of RoeLee the login-in to experiments will be changed to show usernames and require a password to be given for the username selected. Passwords will be extended to up to 20 characters. Usernames will be extended to up to 30 characters. These usernames will then be used as the electronic signature for that user.

In current RoeLee there is the possibility to enter RoeLee in "Read Only" mode without having a password or a username. This mode is useful for statisticians who are concerned with analysing a study without making changes to the study. However, under the new requirements we must know who is generating a given report, and so we will ensure that all users have usernames assigned to them.

We will also introduce the concept of disabling user names. Note that there is a possibility that the Main User name could be disabled, thus effectively completely locking up an experiment.

2. Data Auditing

In RoeLee pre-ratification (that is before we have signed off an animal) we keep only a simple log file containing changes to the data on animals. We now intend to keep total track of data from initial entry to creation of report. A new creation data audit file will be created which will hold the date, time and user number (which relates directly to the relevant user name) for the creation of each item of data. We will then silently audit every change to data before the animal is signed off and fully audit any changes after the animal has been signed off.

Currently , when fully auditing any changes we only require that the user gives a reason for the change. In our reading of Part 11 it is now necessary for the user to sign-off each change as well and thus we have extended the audit procedure to add in provision for the users to enter their password as well as the reason for the change.

3. Signing Off Animals

Currently, in addition to signing off a single animal, we allow users to sign off a whole experiment at once. This seems to go against the spirit of Part 11, so we will stop this possibility and we will also now require a password entered for each animal that is signed off. We will also enhance the audits by adding the time as well as the date that the animal was signed off. We will also add the user number instead of assuming that it was the main user.

This adding of password control after already signing onto an experiment seems to be over cautious, but it does prevent serious changes being made to databases in situations where users have temporarily left their computers and not closed or protected their systems.

To aid users in signing off animals we are also enhancing the facility to complete an animal in data entry option 8, "one animal one, organ at a time" mode. Currently pressing <F12> finishes data entry for an animal, filling in all remaining not entered data as "lesion not present". We will now also offer the users the option to validation, report and sign-off the animal at this stage.

4. Reporting Audits

Once we are recording the complete history of data items it is necessary to develop a way of reporting the information. We are adding a "LIST /AUDIT" facility that will show the current value for a field, its date of creation (with time and user number), all audits done on the field (with date/time/user number) and date/time/user of sign-off.

We are a little unclear from Part 11 when we have to show such information. We have decided to introduce a "REPORT /RAW" option which will show creation and audits on a per-animal basis. Since we will be signing off on a per-animal basis this seems to agree with the requirements of Part 11. We do not feel that Part 11 requires us to give a complete history of all the data points as a footnote to each statistical table produced. Whether the REPORT /RAW should be the only possibility when reporting animals we feel should be left to the client and their interpretation of Part 11. Users will be able set this via the system options.

5. Owners of Reports

Currently users can add their own footnotes declaring who was the principal investigator and who generated the report. The results are output in RTF form and users can then add their own password protection to those files. From our reading of Part 11 we should go further. We are introducing extra footers which force the name of the principal investigator and the generator of the report to be shown. These lines are also shown on the screen whenever a report is produced interactively. When we write these reports away as RTF files, the files are immediately shown as Word files and the user is instructed to give a password to protect the file. This procedure should ensure that where

a report has a password, that report is owned by the person entering that password and that they and the FDA can be certain that no-one else has interfered with the report.

6. File Security

Single pathologists working with their own computers can set up systems to secure their data, even if it just means locking a door. In large companies the basic user files are always open to abuse by determined hackers. In order to secure the files in all cases it has been decided to adopt MD5 checksums on all system files. Users will then be informed if any changes have taken place on the files and be able to take appropriate action, such as going to a back-up version of the files. The one case where it may be appropriate to continue with caution is where a system shut down has occurred whilst some files were still open.

7. Time Limits for Passwords

Some organisations seem to require that passwords are changed at regular intervals. We will therefore enhance the system to allow for a time limit for passwords when required.

8. Running Command Files

Currently no password control is necessary to run a command files through the system. As we need to know the name of the user who is running the command file it will now be necessary for the users to go through the username and password screen before running a command file.

9. Conclusion

RoeLee is a continually evolving system and though we feel that the above changes are a suitable response to the Part 11 requirements others may feel that more work is needed. We welcome any considered comments on this document.

Appendix I

Specification of Audit Trail
Dr.J.S.Fry, 28th November 1984

1. Passwords & Usernames

At entry to program for a new experiment, users supply an experiment name - which will be unalterable. A 9-character password is then asked for. This will become the main password for the experiment. It will be reshown to the user who will be asked to confirm it. If not confirmed, the password will again be asked for. Once confirmed, a 12-character Username will be asked for. This will be used to mark alterations to data on the audit trail for changes made to data. All passwords and usernames will be unalterable, so they will need to be confirmed.

When returning to this experiment once again, the experiment name is entered and a password asked for. There are 3 possibilities here:

1. Main password entered: program entered as per normal - full permissions for user.
2. Old, not main, password entered. Program entered with permissions as from password set-up (see 3).
3. New password entered :-

After confirmation, program asks if new user to be set up. If 'yes' program asks for username and 1 of 3 levels of permission:

1. Read Only. Data can be read and analysed but cannot be altered or added to.
2. Insert Only. Data can be read, analysed, new data entered and new organs and fields can be created. No old data can be overwritten or fields/organs deleted.
3. Full Permissions. All data/fields/organs can be rewritten or deleted. If levels 2 or 3 are wanted, a confirmatory password is needed - this will be the main password.

2. Changes before Ratification

(N.B. We distinguish between validation - as currently in ROELEE 84 - which checks that data satisfy certain defined criteria, and ratification, which is when the pathologist decides the data are final as far as he is concerned, and from which stage there is a GLP requirement to record reasons for changes to the data.)
Before animals/organs have been ratified changes made to data will be put on the log file as at present, except that now a username will be automatically added.

3. Ratifying animals/organs

This will only be possible for users with full permissions. It will be done by data entry option 7. This will first ask: Ratify animals or organs (or non-protocol organs) ?

(i) Animals

Users will select animals either by a SELECT or by a FOR statement.

For each animal chosen the individual animal report will be created. The first page will be shown on the screen. Users will be asked:

1. Show next or previous page of report if it exists.
2. Send report to printer.
3. Go to next animal without ratifying this animal.
4. Leave ratification process altogether.
5. Validate this animal before ratification.

Ratification can only be done after using option 5. When this option is chosen the data for the animal will first be validated. Any errors found will be shown in short on the screen and in full on the printer. The program will then go onto the next animal without allowing the ratification of the present animal.

If no errors are found (or only warnings), users then have the option of ratifying the animal.

Note: Once ratified an animal cannot be unratified.

(ii) Protocol Organs

Protocol organs may be ratified over treatment groups. Users will be asked to supply:

1 : a list of organs - listed by position or short name
(N.B. the program will also be altered so that organ lists can be entered generally by short name as well as position number)
2 : a list of group levels - as for a FOR specification: 1, 3, 5 = groups one, three and five.

The program will then go through each organ in turn, first showing the full organ name and asking users to confirm that it is to be ratified. Within each organ, the program goes through each group in turn, showing the full group level name and asking users to confirm that it is to be ratified.

Then for all animals with that group level, the individual animal reports will be created for just the specified organ. The first screen of reports will be shown to the users who will then be able to:

1. Show next or previous page of reports if it exists.
2. Send reports to printer.
3. Go to next group without ratifying this group.
4. Go to next organ without ratifying this or subsequent groups.
5. Leave ratification process altogether.
6. Validate this organ/group before ratification.

As before ratification can only be done following option 6. If the validation process shows no logical errors for that organ/group, then users can ratify that organ/group and go to the next group for that organ.

(ii) Non-Protocol Organs (if required)
Analagous to (ii) except that no list of organs is specified, all non-protocol organs being considered at once.

4. Changes after Ratification

No field/organ can be deleted after ratification of any animal. No field can be deleted for an organ that is ratified. Any new fields created for new or existing organs will have values automatically set to 0 (not present) for any ratified organ/animal.

When data are altered for a ratified animal, users will be asked to give a reason by means of a grading system with 10 levels - the string this generates will be shown to users for confirmation. Level 10 is 'other' and will ask for 30 characters of free text from users. This can be edited at that point, but no other. When a reason is entered, it becomes the default reason for the next reason, obtainable by hitting carriage return. This will include the free text if option 10 is being used.

The old value, new value, date, username and reason for change will then be entered onto the Audit Log file. This will be a scrambled direct access file, printable only from the program. If, for some reason, the appropriate Audit Log file disappears, the system will generate a rude message when the experiment is entered and only allow 'read only' access to the files.

Appendix II
Amendment of the Code of Federal Regulations by adding Part 11

13464 Federal Register / Vol. 62, No. 54 / Thursday, March 20, 1997 / Rules and Regulations

PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A—General Provisions

Subpart B—Electronic Records

Subpart C—Electronic Signatures

Authority: Secs. 201–903 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321–393); sec. 351 of the Public Health Service Act (42 U.S.C. 262).

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.

§ 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.

§ 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.

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.
(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.
(d) Limiting system access 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.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
(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.
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
(k) Use of appropriate controls over systems documentation including:
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

§ 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.

§ 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).

§ 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.

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.

§ 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.

§ 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.

Dated: March 11, 1997.
William B. Schultz,
Deputy Commissioner for Policy.
[FR Doc. 97–6833 Filed 3–20–97; 8:45 am]
BILLING CODE 4160–01–F