



CERNER CORPORATION
2800 ROCKCREEK PARKWAY
KANSAS CITY, MO 64117-2551
816 201-1024 PHONE
816 474-1742 FAX

June 23, 2004

Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Re: FDA Docket No. 2004N-0133
21 CFR Part 11 Comments

Dear Sir or Madam:

We would like to thank the Agency for soliciting comments regarding 21 CFR Part 11. On the pages that follow, please find 2 copies of Cerner's comments related to Docket No. 2004N-0133.

Sincerely,

A handwritten signature in cursive script that reads "Sandy Adams".

Sandy Adams
Regulatory Affairs Specialist
Cerner Corporation
Phone (816)201-2507
Fax (816)571-2507
Email sadams2@cerner.com

2004N-0133

C12



21 CFR Part 11 Comments to FDA

Regarding: FDA Docket No. 2004N-0133

A. Part 11 Subpart A--General Provisions

Within the context of subpart A of Part 11, we would like interested parties to address the following:

1. We are interested in comments on FDA's interpretation of the narrow scope of Part 11 as discussed in the Part 11 guidance and whether Part 11 should be revised to implement the narrow interpretation described in the guidance.

We agree with the Agency's intent to adopt a narrow scope for Part 11.

2. We are interested in comments on whether revisions to definitions in Part 11 would help clarify a narrow approach and suggestions for any such revisions.

Yes, we would like the Agency to revise the definitions section in Part 11 to help clarify the narrow approach.

3. In the Part 11 guidance we announced that we did not intend to take enforcement action to enforce compliance with the validation, audit trail, record retention, and record copying requirements of part 11 in the manner described in the Part 11 guidance. We emphasized that records must still be maintained or submitted in accordance with the underlying predicate rules, and the agency could take regulatory action for noncompliance with such predicate rules. We are interested in comments on the need for clarification in Part 11 regarding which records are required by predicate rules and are therefore required to be Part 11 compliant?

Yes, we would like the Agency to clarify which records are required by predicate rules and therefore must be Part 11 compliant.

B. Part 11 Subpart B--Electronic Records

Within the context of subpart B, the agency wants to solicit ideas on how to ensure that controls to safeguard records are appropriate and reasonable. There may be instances where persons believe that there are acceptable alternative approaches for implementing controls, with appropriate justification. We want to solicit ideas about how decisions for using alternative controls should be made, such as using a risk assessment.

We would like interested parties to address the following:

1. As mentioned previously, the Part 11 guidance identified four areas where we do not intend to take enforcement action under the circumstances described in the Part 11 guidance, including the validation, audit trail, record retention, and record copying requirements of Part 11. The Part 11 guidance further recommends that decisions on whether or not to implement Part 11 requirements on validation, audit trail, record retention, and record copying



should be based on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity. We are interested in comments on whether there are other areas of Part 11 that should incorporate the concept of a risk-based approach, detailed in the Part 11 guidance (e.g., those that require operational system and device checks).

2. Is additional clarity needed regarding how predicate rule requirements related to subpart B can be fulfilled?

Yes, we agree it would be helpful if the Agency could clarify or provides guidance as to how predicate rule requirements for subpart B can be adequately fulfilled.

3. Under the current Part 11, the controls that apply to electronic records that are maintained also apply to electronic records that are submitted to FDA. Should the requirements for electronic records submitted to FDA be separate from electronic records maintained to satisfy predicate rule requirements?

Yes, it is our opinion that there should be a clear distinction by the Agency between requirements for electronic records submitted to FDA versus those for electronic records maintained to satisfy predicate rules. We would also like to see some reconciliation between Part 11 and the HIPAA Security Rule, and a decision as to whether the electronic signature requirements originally in the draft HIPAA Security Rule will be replaced with Part 11.

4. The controls for electronic records in subpart B distinguish between open systems (an environment where system access is not controlled by persons who are responsible for the content of electronic records that are on the system) and closed systems (an environment where system access is controlled by persons who are responsible for the content of electronic records that are on the system). Should Part 11 continue to differentiate between open systems and closed systems?

Yes, it is our opinion that due to the different levels of security control organizations have over open versus closed systems, the Agency should continue to differentiate between the two when it comes to Part 11. We also would like the Agency to give greater clarification by example of what is a closed system versus an open system.

For individual controls in subpart B, we request comments on the following:

1. The Part 11 guidance identified validation as one of the four areas where we intend to exercise enforcement discretion in the manner described in the guidance. Should we retain the validation provision under Sec. 11.10(b) as required to ensure that a system meets predicate rule requirements for validation?

Yes, it is our opinion that the validation provision is integral to compliance and should be maintained as required. If the Agency does not intend to require or enforce this provision it should be removed.



2. The Part 11 guidance identified record retention and record copying requirements as areas where we plan to exercise enforcement discretion in the manner described in the Part 11 guidance. Are there any related predicate rule requirements that you believe are necessary to preserve the content and meaning of records with respect to record copying and record retention? What requirements would preserve record security and integrity and ensure that records are suitable for inspection, review, and copying by the agency?

Design history file and device master record retention requirements (life of the product plus 2 years) should be taken into consideration when the Agency reviews the record copying and record retention parameters for Part 11. Additionally, the retention requirements of Part 11 should reconcile with the retention requirements under the HIPAA Privacy and Security Rules.

3. Should audit trail requirements include safeguards designed and implemented to deter, prevent, and document unauthorized record creation, modification, and deletion?

Yes, our opinion is that it would be beneficial for the Agency to require safeguards to deter, prevent, and document unauthorized creation, modification and deletion of records.

4. Section 11.10(k) requires appropriate controls over systems documentation. In light of how technology has developed since Part 11 became effective, should Part 11 be modified to incorporate concepts, such as configuration and document management, for all of a system's software and hardware?

C. Part 11 Subpart C--Electronic Signatures

Within the context of subpart C, we would like interested parties to address the following: Section 11.10(d) requires that system access be limited to authorized individuals, but it does not address the handling of security breaches where an unauthorized individual accesses the system. Should Part 11 address investigations and follow-up when these security breaches occur?

It is our opinion that the Agency should add security breach investigation and follow-up requirements to Part 11. Perhaps the Agency could mirror the security breach investigation and curing requirements contained in the HIPAA Security Rule, or just cross-reference these requirements from the Part 11 final Rule.

D. Additional Questions for Comment

In addition, we invite comment on the following questions:

1. What are the economic ramifications of modifying Part 11 based on the issues raised in this document?

It is our opinion that going forward with a narrow scope for Part 11, remaining technology neutral, maintaining a broad definition of electronic signature, and exercising lenient enforcement discretion for legacy systems are all key factors for keeping implementation costs down and avoiding negative economic ramifications. A harmonizing of requirements with the Security Rule would enable organizations to



leverage investments already planned or completed for the Security Rule requirements.

2. Is there a need to clarify in Part 11 which records are required by predicate rules where those records are not specifically identified in predicate rules? If so, how could this distinction be made?

Yes, we agree there is a need for clarification as to which records are required by predicate rules but not specifically identified in predicate rules. Perhaps this distinction could be clarified in a tabular format in the preamble of the modified Part 11 regulation.

3. In what ways can Part 11 discourage innovation?

It is our opinion that Part 11 should remain technology neutral so as not to deter innovation. The definition of electronic signature should be as broad as possible to not limit industry to a particular signing method. The Agency should focus on statement of functional and technical requirements and not specify a solution or method that must be followed.

4. What potential changes to Part 11 would encourage innovation and technical advances consistent with the agency's need to safeguard public health?

The definition of electronic signature in the regulation could be expanded to include (but not require) newer signature technologies. Removal of the filing requirement with FDA for notice of intent to use electronic signatures should be considered by the Agency, since this adds administrative overhead and perhaps discourages some organizations from moving to electronic signature.

5. What risk-based approaches would help to ensure that electronic records have the appropriate levels of integrity and authenticity elements so that electronic signatures are legally binding and authentic?

Some examples of methods to ensure integrity and authenticity would include the following:

- Secure signature management (secure secret store and if digital, secure certificate store/management)*
- Ensuring document succession and signature management are integrated so that the awareness of the need for new signature is understood, and the integrity of the relationship between an instance of a document and the signature is maintained historically for the previously signed versions*
- Secure registration authority and certificate authority functions so that the granting authority for the user/signatory are managed and subject to authorization policies*

6. The Part 11 guidance announced that the agency would exercise enforcement discretion (during our re-examination of Part 11) with respect to all Part 11 requirements for systems that otherwise were operational prior to August 20, 1997 (legacy systems), the effective date of Part 11. What are stakeholder concerns in regards to modifications made to legacy systems in use as of



August 1997? Can the use of risk mitigation and appropriate controls eliminate concerns regarding legacy systems?

We agree with the Agency's decision to exercise enforcement discretion and your intention to not take (or recommend) action to enforce any part 11 requirements with regard to legacy systems. The cost and technological challenges of making these systems Part 11 compliant would be quite onerous.

7. Should Part 11 address record conversion?

The Agency should anticipate the circumstance of conversion from a legacy system to one covered by the Part 11 regulation, and specify any data requirements for ensuring integrity in such a situation.

8. Are there provisions of Part 11 that should be augmented, modified, or deleted as a result of new technologies that have become available since Part 11 was issued?

We would ask that the Agency consider how to modify Part 11 to facilitate signature queuing capabilities, whereby users can review a series of documents and indicate their approval with one electronic signing action, while still maintaining the intent and spirit of the regulation. As with other requirements, this queuing capability should remain technology neutral.



21 CFR Part 11 Comments to FDA

Regarding: FDA Docket No. 2004N-0133

A. Part 11 Subpart A--General Provisions

Within the context of subpart A of Part 11, we would like interested parties to address the following:

1. We are interested in comments on FDA's interpretation of the narrow scope of Part 11 as discussed in the Part 11 guidance and whether Part 11 should be revised to implement the narrow interpretation described in the guidance.

We agree with the Agency's intent to adopt a narrow scope for Part 11.

2. We are interested in comments on whether revisions to definitions in Part 11 would help clarify a narrow approach and suggestions for any such revisions.

Yes, we would like the Agency to revise the definitions section in Part 11 to help clarify the narrow approach.

3. In the Part 11 guidance we announced that we did not intend to take enforcement action to enforce compliance with the validation, audit trail, record retention, and record copying requirements of part 11 in the manner described in the Part 11 guidance. We emphasized that records must still be maintained or submitted in accordance with the underlying predicate rules, and the agency could take regulatory action for noncompliance with such predicate rules. We are interested in comments on the need for clarification in Part 11 regarding which records are required by predicate rules and are therefore required to be Part 11 compliant?

Yes, we would like the Agency to clarify which records are required by predicate rules and therefore must be Part 11 compliant.

B. Part 11 Subpart B--Electronic Records

Within the context of subpart B, the agency wants to solicit ideas on how to ensure that controls to safeguard records are appropriate and reasonable. There may be instances where persons believe that there are acceptable alternative approaches for implementing controls, with appropriate justification. We want to solicit ideas about how decisions for using alternative controls should be made, such as using a risk assessment.

We would like interested parties to address the following:

1. As mentioned previously, the Part 11 guidance identified four areas where we do not intend to take enforcement action under the circumstances described in the Part 11 guidance, including the validation, audit trail, record retention, and record copying requirements of Part 11. The Part 11 guidance further recommends that decisions on whether or not to implement Part 11 requirements on validation, audit trail, record retention, and record copying



should be based on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity. We are interested in comments on whether there are other areas of Part 11 that should incorporate the concept of a risk-based approach, detailed in the Part 11 guidance (e.g., those that require operational system and device checks).

2. Is additional clarity needed regarding how predicate rule requirements related to subpart B can be fulfilled?

Yes, we agree it would be helpful if the Agency could clarify or provides guidance as to how predicate rule requirements for subpart B can be adequately fulfilled.

3. Under the current Part 11, the controls that apply to electronic records that are maintained also apply to electronic records that are submitted to FDA. Should the requirements for electronic records submitted to FDA be separate from electronic records maintained to satisfy predicate rule requirements?

Yes, it is our opinion that there should be a clear distinction by the Agency between requirements for electronic records submitted to FDA versus those for electronic records maintained to satisfy predicate rules. We would also like to see some reconciliation between Part 11 and the HIPAA Security Rule, and a decision as to whether the electronic signature requirements originally in the draft HIPAA Security Rule will be replaced with Part 11.

4. The controls for electronic records in subpart B distinguish between open systems (an environment where system access is not controlled by persons who are responsible for the content of electronic records that are on the system) and closed systems (an environment where system access is controlled by persons who are responsible for the content of electronic records that are on the system). Should Part 11 continue to differentiate between open systems and closed systems?

Yes, it is our opinion that due to the different levels of security control organizations have over open versus closed systems, the Agency should continue to differentiate between the two when it comes to Part 11. We also would like the Agency to give greater clarification by example of what is a closed system versus an open system.

For individual controls in subpart B, we request comments on the following:

1. The Part 11 guidance identified validation as one of the four areas where we intend to exercise enforcement discretion in the manner described in the guidance. Should we retain the validation provision under Sec. 11.10(b) as required to ensure that a system meets predicate rule requirements for validation?

Yes, it is our opinion that the validation provision is integral to compliance and should be maintained as required. If the Agency does not intend to require or enforce this provision it should be removed.



2. The Part 11 guidance identified record retention and record copying requirements as areas where we plan to exercise enforcement discretion in the manner described in the Part 11 guidance. Are there any related predicate rule requirements that you believe are necessary to preserve the content and meaning of records with respect to record copying and record retention? What requirements would preserve record security and integrity and ensure that records are suitable for inspection, review, and copying by the agency?

Design history file and device master record retention requirements (life of the product plus 2 years) should be taken into consideration when the Agency reviews the record copying and record retention parameters for Part 11. Additionally, the retention requirements of Part 11 should reconcile with the retention requirements under the HIPAA Privacy and Security Rules.

3. Should audit trail requirements include safeguards designed and implemented to deter, prevent, and document unauthorized record creation, modification, and deletion?

Yes, our opinion is that it would be beneficial for the Agency to require safeguards to deter, prevent, and document unauthorized creation, modification and deletion of records.

4. Section 11.10(k) requires appropriate controls over systems documentation. In light of how technology has developed since Part 11 became effective, should Part 11 be modified to incorporate concepts, such as configuration and document management, for all of a system's software and hardware?

C. Part 11 Subpart C--Electronic Signatures

Within the context of subpart C, we would like interested parties to address the following: Section 11.10(d) requires that system access be limited to authorized individuals, but it does not address the handling of security breaches where an unauthorized individual accesses the system. Should Part 11 address investigations and follow-up when these security breaches occur?

It is our opinion that the Agency should add security breach investigation and follow-up requirements to Part 11. Perhaps the Agency could mirror the security breach investigation and curing requirements contained in the HIPAA Security Rule, or just cross-reference these requirements from the Part 11 final Rule.

D. Additional Questions for Comment

In addition, we invite comment on the following questions:

1. What are the economic ramifications of modifying Part 11 based on the issues raised in this document?

It is our opinion that going forward with a narrow scope for Part 11, remaining technology neutral, maintaining a broad definition of electronic signature, and exercising lenient enforcement discretion for legacy systems are all key factors for keeping implementation costs down and avoiding negative economic ramifications. A harmonizing of requirements with the Security Rule would enable organizations to



leverage investments already planned or completed for the Security Rule requirements.

2. Is there a need to clarify in Part 11 which records are required by predicate rules where those records are not specifically identified in predicate rules? If so, how could this distinction be made?

Yes, we agree there is a need for clarification as to which records are required by predicate rules but not specifically identified in predicate rules. Perhaps this distinction could be clarified in a tabular format in the preamble of the modified Part 11 regulation.

3. In what ways can Part 11 discourage innovation?

It is our opinion that Part 11 should remain technology neutral so as not to deter innovation. The definition of electronic signature should be as broad as possible to not limit industry to a particular signing method. The Agency should focus on statement of functional and technical requirements and not specify a solution or method that must be followed.

4. What potential changes to Part 11 would encourage innovation and technical advances consistent with the agency's need to safeguard public health?

The definition of electronic signature in the regulation could be expanded to include (but not require) newer signature technologies. Removal of the filing requirement with FDA for notice of intent to use electronic signatures should be considered by the Agency, since this adds administrative overhead and perhaps discourages some organizations from moving to electronic signature.

5. What risk-based approaches would help to ensure that electronic records have the appropriate levels of integrity and authenticity elements so that electronic signatures are legally binding and authentic?

Some examples of methods to ensure integrity and authenticity would include the following:

- Secure signature management (secure secret store and if digital, secure certificate store/management)*
- Ensuring document succession and signature management are integrated so that the awareness of the need for new signature is understood, and the integrity of the relationship between an instance of a document and the signature is maintained historically for the previously signed versions*
- Secure registration authority and certificate authority functions so that the granting authority for the user/signatory are managed and subject to authorization policies*

6. The Part 11 guidance announced that the agency would exercise enforcement discretion (during our re-examination of Part 11) with respect to all Part 11 requirements for systems that otherwise were operational prior to August 20, 1997 (legacy systems), the effective date of Part 11. What are stakeholder concerns in regards to modifications made to legacy systems in use as of



August 1997? Can the use of risk mitigation and appropriate controls eliminate concerns regarding legacy systems?

We agree with the Agency's decision to exercise enforcement discretion and your intention to not take (or recommend) action to enforce any part 11 requirements with regard to legacy systems. The cost and technological challenges of making these systems Part 11 compliant would be quite onerous.

7. Should Part 11 address record conversion?

The Agency should anticipate the circumstance of conversion from a legacy system to one covered by the Part 11 regulation, and specify any data requirements for ensuring integrity in such a situation.

8. Are there provisions of Part 11 that should be augmented, modified, or deleted as a result of new technologies that have become available since Part 11 was issued?

We would ask that the Agency consider how to modify Part 11 to facilitate signature queuing capabilities, whereby users can review a series of documents and indicate their approval with one electronic signing action, while still maintaining the intent and spirit of the regulation. As with other requirements, this queuing capability should remain technology neutral.