same procedure commonly used on paper documents, noted as "X for Y."

92. Proposed § 11.10(k) states that procedures and controls for closed systems must include the use of appropriate systems documentation controls, including: (1) Adequate controls over the distribution, access to, and use of documentation for system operation and maintenance; and (2) records revision and change control procedures to maintain an electronic audit trail that documents time-sequenced development and modification of records. Several comments requested clarification of the type of documents covered by proposed § 11.10(k). One comment noted that this section failed to address controls for record retention. Some comments suggested limiting the scope of systems documentation to application and configurable software, or only to software that could compromise system security or integrity. Other comments suggested that this section should be deleted because some documentation needs wide distribution within an organization, and that it is an onerous burden to control user manuals.

The agency advises that § 11.10(k) is intended to apply to systems documentation, namely, records describing how a system operates and is maintained, including standard operating procedures. The agency believes that adequate controls over such documentation are necessary for various reasons. For example, it is important for employees to have correct and updated versions of standard operating and maintenance procedures. If this documentation is not current, errors in procedures and/or maintenance are more likely to occur. Part 11 does not limit an organization's discretion as to how widely or narrowly any document is to be distributed, and FDA expects that certain documents will, in fact, be widely disseminated. However, some highly sensitive documentation, such as instructions on how to modify system security features, would not routinely be widely distributed. Hence, it is important to control distribution of, access to, and use of such documentation.

Although the agency agrees that the most critical types of system documents would be those directly affecting system security and integrity, FDA does not agree that control over system documentation should only extend to security related software or to application or configurable software. Documentation that relates to operating systems, for example, may also have an impact on security and day-to-day operations. The agency does not agree that it is an onerous burden to control documentation that relates to effective operation and security of electronic records systems. Failure to control such documentation, as discussed above, could permit and foster records falsification by making the enabling instructions for these acts readily available to any individual.

93. Concerning the proposed requirement for adequate controls over documentation for system operation and maintenance, one comment suggested that it be deleted because it is under the control of system vendors, rather than operating organizations. Several comments suggested that the proposed provision be deleted because it duplicates § 11.10(e) with respect to audit trails. Some comments also objected to maintaining the change control procedures in electronic form and suggested deleting the word "electronic" from "electronic audit trails."

The agency advises that this section is intended to apply to systems documentation that can be changed by individuals within an organization. If systems documentation can only be changed by a vendor, this provision does not apply to the vendor's customers. The agency acknowledges that systems documentation may be in paper or electronic form. Where the documentation is in paper form, an audit trail of revisions need not be in electronic form. Where systems documentation is in electronic form, however, the agency intends to require the audit trail also be in electronic form, in accordance with § 11.10(e). The agency acknowledges that, in light of the comments, the proposed rule may not have been clear enough regarding audit trails addressed in § 11.10(k) compared to audit trails addressed in § 11.10(e) and has revised the final rule to clarify this matter.

The agency does not agree, however, that the audit trail provisions of § 11.10(e) and (k), as revised, are entirely duplicative. Section 11.10(e) applies to electronic records in general (including systems documentation); § 11.10(k) applies exclusively to systems documentation, regardless of whether such documentation is in paper or electronic form.

As revised, § 11.10(k) now reads as follows:

(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.

VIII. Electronic Records—Controls for Open Systems (§ 11.30)

Proposed § 11.30 states that: "Open systems used to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity and confidentiality of electronic records from the point of their creation to the point of their receipt." In addition, § 11.30 states:

* * * Such procedures and controls shall include those identified in § 11.10, as appropriate, and such additional measures as document encryption and use of established digital signature standards acceptable to the agency, to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

94. One comment suggested that the reference to digital signature standards be deleted because the agency should not be setting standards and should not dictate how to ensure record authenticity, integrity, and confidentiality. Other comments requested clarification of the agency's expectations with regard to digital signatures: (1) The kinds that would be acceptable, (2) the mechanism for announcing which standards were acceptable (and whether that meant FDA would be certifying particular software), and (3) a definition of digital signature. One comment asserted that FDA should accept international standards for digital signatures. Some comments also requested a definition of encryption. One comment encouraged the agency to further define open systems.

The agency advises that § 11.30 requires additional controls, beyond those identified in § 11.10, as needed under the circumstances, to ensure record authenticity, integrity, and confidentiality for open systems. Use of digital signatures is one measure that may be used, but is not specifically required. The agency wants to ensure that the digital signature standard used is, in fact, appropriate. Development of digital signature standards is a complex undertaking, one FDA does not expect to be performed by individual firms on an ad hoc basis, and one FDA does not now seek to perform.

The agency is nonetheless concerned that such standards be robust and secure. Currently, the agency is aware of two such standards, the RSA (Rivest-Shamir-Adleman), and NIST's Digital Signature Standard (DSS). The DSS became Federal Information Processing Standard (FIPS) 186 on December 1, 1994. These standards are incorporated in different software programs. The agency does not seek to certify or otherwise approve of such programs,

but expects people who use such programs to ensure that they are suitable for their intended use. FDA is aware that NIST provides certifications regarding mathematical conformance to the DSS core algorithms, but does not formally evaluate the broader programs that contain those algorithms. The agency has revised the final rule to clarify its intent that firms retain the flexibility to use any appropriate digital signature as an additional system control for open systems. FDA is also including a definition of digital signature under § 11.3(b)(5).

The agency does not believe it necessary to codify the term "encryption" because, unlike the term digital signature, it has been in general use for many years and is generally understood to mean the transforming of a writing into a secret code or cipher. The agency is aware that there are several commercially available software programs that implement both digital signatures and encryption.

95. Two comments noted that use of digital signatures and encryption is not necessary in the context of PDMA, where access to an electronic record is limited once it is signed and stored. One of the comments suggested that proposed § 11.30 be revised to clarify this point.

As discussed in comment 94 of this document, use of digital signatures and encryption would be an option when extra measures are necessary under the circumstances. In the case of PDMA records, such measures may be warranted in certain circumstances, and unnecessary in others. For example, if electronic records were to be transmitted by a firm's representative by way of a public online service to a central location, additional measures would be necessary. On the other hand, where the representative's records are hand delivered to that location, or transferred by direct connection between the representative and the central location, such additional measures to ensure record authenticity, confidentiality, and integrity may not be necessary. The agency does not believe that it is practical to revise § 11.30 to elaborate on every possible situation in which additional measures would or would not be needed.

96. One comment addressed encryption of submissions to FDA and asked if people making those submissions would have to give the agency the appropriate "keys" and, if so, how the agency would protect the security of such information.

The agency intends to develop appropriate procedures regarding the exchange of "keys" attendant to use of encryption and digital signatures, and will protect those keys that must remain confidential, in the same manner as the agency currently protects trade secrets. Where the agency and a submitter agree to use a system that calls for the exchange of secret keys, FDA will work with submitters to achieve mutually agreeable procedures. The agency notes, however, that not all encryption and digital signature systems require that enabling keys be secret.

97. One comment noted that proposed § 11.30 does not mention availability and nonrepudiation and requested clarification of the term "point of receipt." The comment noted that, where an electronic record is received at a person's electronic mailbox (which resides on an open system), additional measures may be needed when the record is transferred to the person's own local computer because such additional transfer entails additional security risks. The comment suggested wording that would extend open system controls to the point where records are ultimately retained.

The agency agrees that, in the situation described by the comment, movement of the electronic record from an electronic mailbox to a person's local computer may necessitate open system controls. However, situations may vary considerably as to the ultimate point of receipt, and FDA believes proposed § 11.30 offers greater flexibility in determining open system controls than revisions suggested by the comment. The agency advises that the concept of nonrepudiation is part of record authenticity and integrity, as already covered by § 11.10(c). Therefore, FDA is not revising § 11.30 as suggested.

IX. Electronic Records—Signature Manifestations (§ 11.50)

Proposed § 11.50 requires that electronic records that are electronically signed must display in clear text the printed name of the signer, and the date and time when the electronic signature was executed. This section also requires that electronic records clearly indicate the meaning (such as review, approval, responsibility, and authorship) associated with their attendant signatures.

98. Several comments suggested that the information required under proposed § 11.50 need not be contained in the electronic records themselves, but only in the human readable format (screen displays and printouts) of such records. The comments explained that the records themselves need only contain links, such as signature attribute codes, to such information to produce the displays of information required. The comments noted, for example, that, where electronic signatures consist of an identification code in combination with a password, the combined code and password itself would not be part of the display. Some comments suggested that proposed § 11.50 be revised to clarify what items are to be displayed.

The agency agrees and has revised proposed § 11.50 accordingly. The intent of this section is to require that human readable forms of signed electronic records, such as computer screen displays and printouts bear: (1) The printed name of the signer (at the time the record is signed as well as whenever the record is read by humans); (2) the date and time of signing; and (3) the meaning of the signature. The agency believes that revised § 11.50 will afford persons the flexibility they need to implement the display of information appropriate for their own electronic records systems, consistent with other system controls in part 11, to ensure record integrity and prevent falsification.

99. One comment stated that the controls in proposed § 11.50 would not protect against inaccurate entries.

FDA advises that the purpose of this section is not to protect against inaccurate entries, but to provide unambiguous documentation of the signer, when the signature was executed, and the signature's meaning. The agency believes that such a record is necessary to document individual responsibility and actions.

In a paper environment, the printed name of the individual is generally present in the signed record, frequently part of a traditional "signature block." In an electronic environment, the person's name may not be apparent, especially where the signature is based on identification codes combined with passwords. In addition, the meaning of a signature is generally apparent in a paper record by virtue of the context of the record or, more often, explicit phrases such as "approved by," "reviewed by," and "performed by." Thus, the agency believes that for clear documentation purposes it is necessary to carry such meanings into the electronic record environment.

100. One comment suggested that proposed § 11.50 should apply only to those records that are required to be signed, and that the display of the date and time should be performed in a secure manner.

The agency intends that this section apply to all signed electronic records regardless of whether other regulations require them to be signed. The agency believes that if it is important enough that a record be signed, human readable

displays of such records must include the printed name of the signer, the date and time of signing, and the meaning of the signature. Such information is crucial to the agency's ability to protect public health. For example, a message from a firm's management to employees instructing them on a particular course of action may be critical in litigation. This requirement will help ensure clear documentation and deter falsification regardless of whether the signature is electronic or handwritten.

The agency agrees that the display of information should be carried out in a secure manner that preserves the integrity of that information. The agency, however, does not believe it is necessary at this time to revise § 11.50 to add specific security measures because other requirements of part 11 have the effect of ensuring appropriate security.

Because signing information is important regardless of the type of signature used, the agency has revised § 11.50 to cover all types of signings.

101. Several comments objected to the requirement in proposed § 11.50(a) that the time of signing be displayed in addition to the date on the grounds that such information is: (1) Unnecessary, (2) costly to implement, (3) needed in the electronic record for auditing purposes, but not needed in the display of the record, and (4) only needed in critical applications. Some comments asserted that recording time should be optional. One comment asked whether the time should be local to the signer or to a central network when electronic record systems cross different time zones.

The agency believes that it is vital to record the time when a signature is applied. Documenting the time when a signature was applied can be critical to demonstrating that a given record was, or was not, falsified. Regarding systems that may span different time zones, the agency advises that the signer's local time is the one to be recorded.

102. One comment assumed that a person's user identification code could be displayed instead of the user's printed name, along with the date and time of signing.

This assumption is incorrect. The agency intends that the printed name of the signer be displayed for purposes of unambiguous documentation and to emphasize the importance of the act of signing to the signer. The agency believes that because an identification code is not an actual name, it would not be a satisfactory substitute.

103. One comment suggested that the word "printed" in the phrase "printed name" be deleted because the word was superfluous. The comment also stated that the rule should state when the clear text must be created or displayed because some computer systems, in the context of electronic data interchange transactions, append digital signatures to records before, or in connection with, communication of the record.

The agency disagrees that the word "printed" is superfluous because the intent of this section is to show the name of the person in an unambiguous manner that can be read by anyone. The agency believes that requiring the printed name of the signer instead of codes or other manifestations, more effectively provides clarity.

The agency has revised this section to clarify the point at which the signer's information must be displayed, namely, as part of any human readable form of the electronic record. The revision, in the agency's view, addresses the comment's concern regarding the application of digital signatures. The agency advises that under § 11.50, any time after an electronic record has been signed, individuals who see the human readable form of the record will be able to immediately tell who signed the record, when it was signed, and what the signature meant. This includes the signer who, as with a traditional signature to paper, will be able to review the signature instantly.

104. One comment asked if the operator would have to see the meaning of the signature, or if the information had to be stored on the physical electronic record.

As discussed in comment 100 of this document, the information required by § 11.50(b) must be displayed in the human readable format of the electronic record. Persons may elect to store that information directly within the electronic record itself, or in logically associated records, as long as such information is displayed any time a person reads the record.

105. One comment noted that proposed § 11.50(b) could be interpreted to require lengthy explanations of the signatures and the credentials of the signers. The comment also stated that this information would more naturally be contained in standard operating procedures, manuals, or accompanying literature than in the electronic records themselves.

The agency believes that the comment misinterprets the intent of this provision. Recording the meaning of the signature does not infer that the signer's credentials or other lengthy explanations be part of that meaning. The statement must merely show what is meant by the act of signing (e.g., review, approval, responsibility, authorship).

106. One comment noted that the meaning of a signature may be included in a (digital signature) public key certificate and asked if this would be acceptable. The comment also noted that the certificate might be easily accessible by a record recipient from either a recognized database or one that might be part of, or associated with, the electronic record itself. The comment further suggested that FDA would benefit from participating in developing rules of practice regarding certificate-based public key cryptography and infrastructure with the Information Security Committee, Section of Science and Technology, of the American Bar Association (ABA).

The intent of this provision is to clearly discern the meaning of the signature when the electronic record is displayed in human readable form. The agency does not expect such meaning to be contained in or displayed by a public key certificate because the public key is generally a fixed value associated with an individual. The certificate is used by the recipient to authenticate a digital signature that may have different meanings, depending upon the record being signed. FDA acknowledges that it is possible for someone to establish different public keys, each of which may indicate a different signature meaning. Part 11 would not prohibit multiple "meaning" keys provided the meaning of the signature itself was still clear in the display of the record, a feature that could conceivably be implemented by software.

Regarding work of the ABA and other standard-setting organizations, the agency welcomes an open dialog with such organizations, for the mutual benefit of all parties, to establish and facilitate the use of electronic record/electronic signature technologies. FDA's participation in any such activities would be in accordance with the agency's policy on standards stated in the Federal Register of October 11, 1995 (60 FR 53078).

Revised § 11.50, signature manifestations, reads as follows:

(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).

X. Electronic Records—Signature/Record Linking (§ 11.70)

107. Proposed § 11.70 states that electronic signatures and handwritten signatures executed to electronic records must be verifiably bound to their respective records to ensure that signatures could not be excised, copied, or otherwise transferred to falsify another electronic record.

Many comments objected to this provision as too prescriptive, unnecessary, unattainable, and excessive in comparison to paper-based records. Some comments asserted that the objectives of the section could be attained through appropriate procedural and administrative controls. The comments also suggested that objectives of the provision could be met by appropriate software (i.e., logical) links between the electronic signatures and electronic records, and that such links are common in systems that use identification codes in combination with passwords. One firm expressed full support for the provision, and noted that its system implements such a feature and that signature-to-record binding is similar to the record-locking provision of the proposed PDMA regulations.

The agency did not intend to mandate use of any particular technology by use of the word "binding." FDA recognizes that, because it is relatively easy to copy an electronic signature to another electronic record and thus compromise or falsify that record, a technology based link is necessary. The agency does not believe that procedural or administrative controls alone are sufficient to ensure that objective because such controls could be more easily circumvented than a straightforward technology based approach. In addition, when electronic records are transferred from one party to another, the procedural controls used by the sender and recipient may be different. This could result in record falsification by signature transfer.

The agency agrees that the word "link" would offer persons greater flexibility in implementing the intent of this provision and in associating the names of individuals with their identification codes/passwords without actually recording the passwords themselves in electronic records. The agency has revised proposed § 11.70 to state that signatures shall be linked to their electronic records.

108. Several comments argued that proposed § 11.70 requires absolute protection of electronic records from falsification, an objective that is unrealistic to the extent that determined individuals could falsify records.

The agency acknowledges that, despite elaborate system controls, certain determined individuals may find a way to defeat antifalsification measures. FDA will pursue such illegal activities as vigorously as it does falsification of paper records. For purposes of part 11, the agency's intent is to require measures that prevent electronic records falsification by ordinary means. Therefore, FDA has revised § 11.70 by adding the phrase "by ordinary means" at the end of this section.

109. Several comments suggested changing the phrase "another electronic record" to "an electronic record" to clarify that the antifalsification provision applies to the current record as well as any other record.

The agency agrees and has revised § 11.70 accordingly.

110. Two comments argued that signature-to-record binding is unnecessary, in the context of PDMA, beyond the point of record creation (i.e., when records are transmitted to a point of receipt). The comments asserted that persons who might be in a position to separate a signature from a record (for purposes of falsification) are individuals responsible for record integrity and thus unlikely to falsify records. The comments also stated that signature-to-record binding is produced by software coding at the time the record is signed, and suggested that proposed § 11.70 clarify that binding would be necessary only up to the point of actual transmission of the electronic record to a central point of receipt.

The agency disagrees with the comment's premise that the need for binding to prevent falsification depends on the disposition of people to falsify records. The agency believes that reliance on individual tendencies is insufficient insurance against falsification. The agency also notes that in the traditional paper record, the signature remains bound to its corresponding record regardless of where the record may go.

111. One comment suggested that proposed § 11.70 be deleted because it appears to require that all records be kept on inalterable media. The comment also suggested that the phrase "otherwise transferred" be deleted on the basis that it should be permissible for copies of handwritten signatures (recorded electronically) to be made when used, in addition to another unique individual identification mechanism.

The agency advises that neither § 11.70, nor other sections in part 11, requires that records be kept on inalterable media. What is required is that whenever revisions to a record are made, the original entries must not be obscured. In addition, this section does not prohibit copies of handwritten signatures recorded electronically from being made for legitimate reasons that do not relate to record falsification. Section 11.70 merely states that such copies must not be made that falsify electronic records.

112. One comment suggested that proposed § 11.70 be revised to require application of response cryptographic methods because only those methods could be used to comply with the regulation. The comment noted that, for certificate based public key cryptographic methods, the agency should address verifiable binding between the signer's name and public key as well as binding between digital signatures and electronic records. The comment also suggested that the regulation should reference electronic signatures in the context of secure time and date stamping.

The agency intends to permit maximum flexibility in how organizations achieve the linking called for in § 11.70, and, as discussed above, has revised the regulation accordingly. Therefore, FDA does not believe that cryptographic and digital signature methods would be the only ways of linking an electronic signature to an electronic document. In fact, one firm commented that its system binds a person's handwritten signature to an electronic record. The agency agrees that use of digital signatures accomplishes the same objective because, if a digital signature were to be copied from one record to another, the second record would fail the digital signature verification procedure. Furthermore, FDA notes that concerns regarding binding a person's name with the person's public key would be addressed in the context of § 11.100(b) because an organization must establish an individual's identity before assigning or certifying an electronic signature (or any of the electronic signature components).

113. Two comments requested clarification of the types of technologies that could be used to meet the requirements of proposed § 11.70.

As discussed in comment 107 of this document, the agency is affording persons maximum flexibility in using any appropriate method to link electronic signatures to their respective electronic records to prevent record falsification. Use of digital signatures is one such method, as is use of software locks to prevent sections of codes

representing signatures from being copied or removed. Because this is an area of developing technology, it is likely that other linking methods will emerge.

XI. Electronic Signatures—General Requirements (§ 11.100)

Proposed § 11.100(a) states that each electronic signature must be unique to one individual and not be reused or reassigned to anyone else.

114. One comment asserted that several people should be permitted to share a common identification code and password where access control is limited to inquiry only.

Part 11 does not prohibit the establishment of a common group identification code/password for read only access purposes. However, such commonly shared codes and passwords would not be regarded, and must not be used, as electronic signatures. Shared access to a common database may nonetheless be implemented by granting appropriate common record access privileges to groups of people, each of whom has a unique electronic signature.

115. Several comments said proposed § 11.100(a) should permit identification codes to be reused and reassigned from one employee to another, as long as an audit trail exists to associate an identification code with a given individual at any one time, and different passwords are used. Several comments said the section should indicate if the agency intends to restrict authority delegation by the nonreassignment or nonreuse provision, or by the provision in § 11.200(a)(2) requiring electronic signatures to be used only by their genuine owners. The comments questioned whether reuse means restricting one noncryptographic based signature to only one record and argued that passwords need not be unique if the combined identification code and password are unique to one individual. One comment recommended caution in using the term "ownership" because of possible confusion with intellectual property rights or ownership of the computer systems themselves.

The agency advises that, where an electronic signature consists of the combined identification code and password, § 11.100 would not prohibit the reassignment of the identification code provided the combined identification code and password remain unique to prevent record falsification. The agency believes that such reassignments are inadvisable, however, to the extent that they might be combined with an easily guessed password, thus increasing the chances that an individual might assume a signature belonging to someone else. The agency also advises that where people can read identification codes (e.g., printed numbers and letters that are typed at a keyboard or read from a card), the risks of someone obtaining that information as part of a falsification effort would be greatly increased as compared to an identification code that is not in human readable form (one that is, for example, encoded on a "secure card" or other device).

Regarding the delegation of authority to use electronic signatures, FDA does not intend to restrict the ability of one individual to sign a record or otherwise act on behalf of another individual. However, the applied electronic signature must be the assignee's and the record should clearly indicate the capacity in which the person is acting (e.g., on behalf of, or under the authority of, someone else). This is analogous to traditional paper records and handwritten signatures when person "A" signs his or her own name under the signature block of person "B," with appropriate explanatory notations such as "for" or "as representative of" person B. In such cases, person A does not simply sign the name of person B. The agency expects the same procedure to be used for electronic records and electronic signatures.

The agency intends the term "reuse" to refer to an electronic signature used by a different person. The agency does not regard as "reuse" the replicate application of a noncryptographic based electronic signature (such as an identification code and password) to different electronic records. For clarity, FDA has revised the phrase "not be reused or reassigned to" to state "not be reused by, or reassigned to," in § 11.100(a).

The reference in § 11.200(a) to ownership is made in the context of an individual owning or being assigned a particular electronic signature that no other individual may use. FDA believes this is clear and that concerns regarding ownership in the context of intellectual property rights or hardware are misplaced.

116. One comment suggested that proposed § 11.100(a) should accommodate electronic signatures assigned to organizations rather than individuals.

The agency advises that, for purposes of part 11, electronic signatures are those of individual human beings and not organizations. For example, FDA does not regard a corporate seal as an individual's signature. Humans may represent and obligate organizations by signing records, however. For clarification, the agency is substituting the word "individual" for "person" in the definition of electronic signature (§ 11.3(b)(7)) because the broader definition of person within the act includes organizations.

117. Proposed § 11.100(b) states that, before an electronic signature is assigned to a person, the identity of the individual must be verified by the assigning authority.

Two comments noted that where people use identification codes in combination with passwords only the identification code portion of the electronic signature is assigned, not the password. Another comment argued that the word "assigned" is inappropriate in the context of electronic signatures based upon public key cryptography because the appropriate authority certifies the bind between the individual's public key and identity, and not the electronic signature itself.

The agency acknowledges that, for certain types of electronic signatures, the authorizing or certifying organization issues or approves only a portion of what eventually becomes an individual's electronic signature. FDA wishes to accommodate a broad variety of electronic signatures and is therefore revising § 11.100(b) to require that an organization verify the identity of an individual before it establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature or any element of such electronic signature.

118. One comment suggested that the word "verified" in proposed § 11.100(b) be changed to "confirmed." Other comments addressed the method of verifying a person's identity and suggested that the section specify acceptable verification methods, including high level procedures regarding the relative strength of that verification, and the need for personal appearances or supporting documentation such as birth certificates. Two comments said the verification provision should be deleted because normal internal controls are adequate, and that it was impractical for multinational companies whose employees are globally dispersed.

The agency does not believe that there is a sufficient difference between "verified" and "confirmed" to warrant a change in this section. Both words indicate that organizations substantiate a person's identity to prevent impersonations when an electronic signature, or any of its elements, is being established or certified. The agency disagrees with the assertion that this requirement is unnecessary. Without verifying someone's identity at the outset of establishing or certifying

an individual's electronic signature, or a portion thereof, an imposter might easily access and compromise many records. Moreover, an imposter could continue this activity for a prolonged period of time despite other system controls, with potentially serious consequences.

The agency does not believe that the size of an organization, or global dispersion of its employees, is reason to abandon this vital control. Such dispersion may, in fact, make it easier for an impostor to pose as someone else in the absence of such verification. Further, the agency does not accept the implication that multinational firms would not verify the identity of their employees as part of other routine procedures, such as when individuals are first hired.

In addition, in cases where an organization is widely dispersed and electronic signatures are established or certified centrally, § 11.100(b) does not prohibit organizations from having their local units perform the verification and relaying this information to the central authority. Similarly, local units may conduct the electronic signature assignment or certification.

FDA does not believe it is necessary at this time to specify methods of identity verification and expects that organizations will consider risks attendant to sanctioning an erroneously assigned electronic signature.

119. Proposed § 11.100(c) states that persons using electronic signatures must certify to the agency that their electronic signature system guarantees the authenticity, validity, and binding nature of any electronic signature. Persons utilizing electronic signatures would, upon agency request, provide additional certification or testimony that a specific electronic signature is authentic, valid, and binding. Such certification would be submitted to the FDA district office in which territory the electronic signature system is in use.

Many comments objected to the proposed requirement that persons provide FDA with certification regarding their electronic signature systems. The comments asserted that the requirement was: (1) Unprecedented, (2) unrealistic, (3) unnecessary, (4) contradictory to the principles and intent of system validation, (5) too burdensome for FDA to manage logistically, (6) apparently intended only to simplify FDA litigation, (7) impossible to meet regarding "guarantees" of authenticity, and (8) an apparent substitute for FDA inspections.

FDA agrees in part with these comments. This final rule reduces the scope and burden of certification to a statement of intent that electronic signatures are the legally binding equivalent of handwritten signatures.

As noted previously, the agency believes it is important, within the context of its health protection activities, to ensure that persons who implement electronic signatures fully equate the legally binding nature of electronic signatures with the traditional handwritten paper-based signatures. The agency is concerned that individuals might disavow an electronic signature as something completely different from a traditional handwritten signature. Such contention could result in confusion and possibly extensive litigation.

Moreover, a limited certification as provided in this final rule is consistent with other legal, regulatory, and commercial practices. For example, electronic data exchange trading partner agreements are often written on paper and signed with traditional handwritten signatures to establish that certain electronic identifiers are recognized as equivalent to traditional handwritten signatures.

FDA does not expect electronic signature systems to be guaranteed foolproof. The agency does not intend, under § 11.100(c), to establish a requirement that is unattainable. Certification of an electronic signature system as the legally binding equivalent of a traditional handwritten signature is separate and distinct from system validation. This provision is not intended as a substitute for FDA inspection and such inspection alone may not be able to determine in a conclusive manner an organization's intent regarding electronic signature equivalency.

The agency has revised proposed § 11.100(c) to clarify its intent. The agency wishes to emphasize that the final rule dramatically curtails what FDA had proposed and is essential for the agency to be able to protect and promote the public health because FDA must be able to hold people to the commitments they make under their electronic signatures. The certification in the final rule is merely a statement of intent that electronic signatures are the legally binding equivalent of traditional handwritten signatures.

120. Several comments questioned the procedures necessary for submitting the certification to FDA, including: (1) The scheduling of the certification; (2) whether to submit certificates for each individual or for each electronic signature; (3) the meaning of "territory" in the context of wide area networks; (4) whether such certificates could be submitted electronically; and (5) whether organizations, after submitting a certificate, had to wait for a response from FDA before implementing their electronic signature systems. Two comments suggested revising proposed § 11.100(c) to require that all certifications be submitted to FDA only upon agency request. One comment suggested changing "should" to "shall" in the last sentence of § 11.100(c) if the agency's intent is to require certificates to be submitted to the respective FDA district office.

The agency intends that certificates be submitted once, in the form of a paper letter, bearing a traditional handwritten signature, at the time an organization first establishes an electronic signature system after the effective date of part 11, or, where such systems have been used before the effective date, upon continued use of the electronic signature system.

A separate certification is not needed for each electronic signature, although certification of a particular electronic signature is to be submitted if the agency requests it. The agency does not intend to establish certification as a review and approval function. In addition, organizations need not await FDA's response before putting electronic signature systems into effect, or before continuing to use an existing system.

A single certification may be stated in broad terms that encompass electronic signatures of all current and future employees, thus obviating the need for subsequent certifications submitted on a preestablished schedule.

To further simplify the process and to minimize the number of certifications that persons would have to provide, the agency has revised § 11.100(c) to permit submission of a single certification that covers all electronic signatures used by an organization. The revised rule also simplifies the process by providing a single agency receiving unit. The final rule instructs persons to send certifications to FDA's Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857. Persons outside the United States may send their certifications to the same office.

The agency offers, as guidance, an example of an acceptable § 11.100(c) certification:

Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that [name of organization] intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures.