equipment" within the meaning of section 704 of the act (21 U.S.C. 374).

The agency does not expect persons to maintain obsolete and supplanted computer systems for the sole purpose of enabling FDA inspection. However, the agency does expect firms to maintain and have available for inspection documentation relevant to those systems, in terms of compliance with part 11, for as long as the electronic records are required by other relevant regulations. Persons should also be mindful of the need to keep appropriate computer systems that are capable of reading electronic records for as long as those records must be retained. In some instances, this may mean retention of otherwise outdated and supplanted systems, especially where the old records cannot be converted to a form readable by the newer systems. In most cases, however, FDA believes that where electronic records are accurately and completely transcribed from one system to another, it would not be necessary to maintain older systems.

31. One comment requested that proposed part 11 be revised to give examples of electronic records subject to FDA inspection, including pharmaceutical and medical device production records, in order to reduce the need for questions.

The agency does not believe that it is necessary to include examples of records it might inspect because the addition of such examples might raise questions about the agency's intent to inspect other records that were not identified.

32. One comment said that the regulation should state that certain security related information, such as private keys attendant to cryptographic implementation, is not intended to be subject to inspection, although procedures related to keeping such keys confidential can be subject to inspection.

The agency would not routinely seek to inspect especially sensitive information, such as passwords or private keys, attendant to security systems. However, the agency reserves the right to conduct such inspections, consistent with statutory limitations, to enforce the provisions of the act and related statutes. It may be necessary, for example, in investigating cases of suspected fraud, to access and determine passwords and private keys, in the same manner as the agency may obtain specimens of handwritten signatures ("exemplars"). Should there be any reservations about such inspections, persons may, of course, change their passwords and private keys after FDA inspection.

33. One comment asked how persons were expected to meet the proposed requirement, under § 11.1(e), that computer systems be readily available for inspection when such systems include geographically dispersed networks. Another comment said FDA investigators should not be permitted to access industry computer systems as part of inspections because investigators would be untrained users.

The agency intends to inspect those parts of electronic record or signature systems that have a bearing on the trustworthiness and reliability of electronic records and electronic signatures under part 11. For geographically dispersed systems, inspection at a given location would extend to operations, procedures, and controls at that location, along with interaction of that local system with the wider network. The agency would inspect other locations of the network in a separate but coordinated manner, much the same way the agency currently conducts inspections of firms that have multiple facilities in different parts of the country and outside of the United States.

FDA does not believe it is reasonable to rule out computer system access as part of an inspection of electronic record or signature systems. Historically, FDA investigators observe the actions of establishment employees, and (with the cooperation of establishment management) sometimes request that those employees perform some of their assigned tasks to determine the degree of compliance with established requirements. However, there may be times when FDA investigators need to access a system directly. The agency is aware that such access will generally require the cooperation of and, to some degree, instruction by the firms being inspected. As new, complex technologies emerge, FDA will need to develop and implement new inspectional methods in the context of those technologies.

V. Implementation (§ 11.2)

34. Proposed § 11.2(a) stated that for "records required by chapter I of this title to be maintained, but not submitted to the agency, persons may use electronic records/signatures in lieu of paper records/conventional signatures, in whole or in part, * * *."

Two comments requested clarification of the term "conventional signatures." One comment suggested that the term "traditional signatures" be used instead. Another suggested rewording in order to clarify the slash in the phrase "records/signatures."

The agency advises that the term "conventional signature" means handwritten signature. The agency agrees that the term "traditional signature" is preferable, and has revised § 11.2(a) and (b) accordingly. The agency has also clarified proposed § 11.2(a) by replacing the slash with the word "or."

35. One comment asked if the term "persons" in proposed § 11.2(b) would include devices because computer systems frequently apply digital time stamps on records automatically, without direct human intervention.

The agency advises that the term "persons" excludes devices. The agency does not consider the application of a time stamp to be the application of a signature.

36. Proposed § 11.2(b)(2) provides conditions under which electronic records or signatures could be submitted to the agency in lieu of paper. One condition is that a document, or part of a document, must be identified in a public docket as being the type of submission the agency will accept in electronic form. Two comments addressed the nature of the submissions to the public docket. One comment asked that the agency provide specifics, such as the mechanism for updating the docket and the frequency of such updates. One comment suggested making the docket available to the public by electronic means. Another comment suggested that acceptance procedures be uniform among agency units and that electronic mail be used to hold consultations with the agency. One comment encouraged the agency units receiving the submissions to work closely with regulated industry to ensure that no segment of industry is unduly burdened and that agency guidance is widely accepted.

The agency intends to develop efficient electronic records acceptance procedures that afford receiving units sufficient flexibility to deal with submissions according to their capabilities. Although agencywide uniformity is a laudable objective, to attain such flexibility it may be necessary to accommodate some differences among receiving units. The agency considers of primary importance, however, that all part 11 submissions be trustworthy, reliable, and in keeping with FDA regulatory activity. The agency expects to work closely with industry to help ensure that the mechanics and logistics of accepting electronic submissions do not pose any undue burdens. However, the agency expects persons to consult with the

intended receiving units on the technical aspects of the submission, such as media, method of transmission, file format, archiving needs, and technical protocols. Such consultations will ensure that submissions are compatible with the receiving units' capabilities. The agency has revised proposed § 11.2(b)(2) to clarify this expectation.

Regarding the public docket, the agency is not at this time establishing a fixed schedule for updating what types of documents are acceptable for submission because the agency expects the docket to change and grow at a rate that cannot be predicted. The agency may, however, establish a schedule for updating the docket in the future. The agency agrees that making the docket available electronically is advisable and will explore this option. Elsewhere in this issue of the Federal Register, FDA is providing further information on this docket.

VI. Definitions (§ 11.3)

37. One comment questioned the incorporation in proposed § 11.3(a) of definitions under section 201 of the act (21 U.S.C. 321), noting that other FDA regulations (such as 21 CFR parts 807 and 820) lack such incorporation, and suggested that it be deleted.

The agency has retained the incorporation by reference to definitions under section 201 of the act because those definitions are applicable to part 11.

38. One comment suggested adding the following definition for the term "digital signature:" "data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient."

The agency agrees that the term digital signature should be defined and has added new § 11.3(b)(5) to provide a definition for digital signature that is consistent with the Federal Information Processing Standard 186, issued May 19, 1995, and effective December 1, 1995, by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST). Generally, a digital signature is "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." FDA advises that the set of rules and parameters is established in each digital signature standard.

39. Several comments suggested various modifications of the proposed definition of biometric/behavioral links, and suggested revisions that would exclude typing a password or identification code which, the comments noted, is a repeatable action. The comments suggested that actions be unique and measurable to meet the intent of a biometric method.

The agency agrees that the proposed definition of biometric/behavioral links should be revised to clarify the agency's intent that repetitive actions alone, such as typing an identification code and password, are not considered to be biometric in nature. Because comments also indicated that it would be preferable to simplify the term, the agency is changing the term "biometric/behavioral link" to "biometrics." Accordingly, § 11.3(b)(3) defines the term "biometrics" to mean "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."

40. One comment said that the agency should identify what biometric methods are acceptable to verify a person's identity and what validation acceptance criteria the agency has used to determine that biometric technologies are superior to other methods, such as use of identification codes and passwords.

The agency believes that there is a wide variety of acceptable technologies, regardless of whether they are based on biometrics, and regardless of the particular type of biometric mechanism that may be used. Under part 11, electronic signatures that employ at least two distinct identification components such as identification codes and passwords, and electronic signatures based on biometrics are equally acceptable substitutes for traditional handwritten signatures. Furthermore, all electronic record systems are subject to the same requirements of subpart B of part 11 regardless of the electronic signature technology being used. These provisions include requirements for validation.

Regarding the comment's suggestion that FDA apply quantitative acceptance criteria, the agency is not seeking to set specific numerical standards or statistical performance criteria in determining the threshold of acceptability for any type of technology. If such standards were to be set for biometrics-based electronic signatures, similar numerical performance and reliability requirements would have to be applied to other technologies as well. The agency advises, however, that the differences between system controls for biometrics-based electronic signatures and other electronic signatures are a result of the premise that biometrics-based electronic signatures, by their nature, are less prone to be compromised than other methods such as identification codes and passwords. Should it become evident that additional controls are warranted for biometrics-based electronic signatures, the agency will propose to revise part 11 accordingly.

41. Proposed § 11.3(b)(4) defined a closed system as an environment in which there is communication among multiple persons, and where system access is restricted to people who are part of the organization that operates the system.

Many comments requested clarification of the term "organization" and stated that the rule should account for persons who, though not strictly employees of the operating organization, are nonetheless obligated to it in some manner, or who would otherwise be granted system access by the operating organization. As examples of such persons, the comments cited outside contractors, suppliers, temporary employees, and consultants. The comments suggested a variety of alternative wording, including a change of emphasis from organizational membership to organizational control over system access. One comment requested clarification of whether the rule intends to address specific disciplines within a company.

Based on the comments, the agency has revised the proposed definition of closed system to state "an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system." The agency agrees that the most important factor in classifying a system as closed or open is whether the persons responsible for the content of the electronic records control access to the system containing those records. A system is closed if access is controlled by persons responsible for the content of the records. If those persons do not control such access, then the system is open because the records may be read, modified, or compromised by others to the possible detriment of the persons responsible for record content. Hence, those responsible for the records would need to take appropriate additional measures in an open system to protect those records from being read, modified, destroyed, or otherwise compromised by unauthorized and potentially unknown parties. The agency does not believe it is necessary to codify the basis or criteria for authorizing system access, such as existence of a fiduciary

responsibility or contractual relationship. By being silent on such criteria, the rule affords maximum flexibility to organizations by permitting them to determine those criteria for themselves.

42. Concerning the proposed definition of closed system, one comment suggested adding the words "or devices" after "persons" because communications may involve nonhuman entities.

The agency does not believe it is necessary to adopt the suggested revision because the primary intent of the regulation is to address communication among humans, not devices.

43. One comment suggested defining a closed system in terms of functional characteristics that include physical access control, having professionally written and approved procedures with employees and supervisors trained to follow them, conducting investigations when abnormalities may have occurred, and being under legal obligation to the organization responsible for operating the system.

The agency agrees that the functional characteristics cited by the comment are appropriate for a closed system, but has decided that it is unnecessary to include them in the definition. The functional characteristics themselves, however, such as physical access controls, are expressed as requirements elsewhere in part 11.

44. Two comments said that the agency should regard as closed a system in which dial-in access via public phone lines is permitted, but where access is authorized by, and under the control of, the organization that operates the system.

The agency advises that dial-in access over public phone lines could be considered part of a closed system where access to the system that holds the electronic records is under the control of the persons responsible for the content of those records. The agency cautions, however, that, where an organization's electronic records are stored on systems operated by third parties, such as commercial online services, access would be under control of the third parties and the agency would regard such a system as being open. The agency also cautions that, by permitting access to its systems by public phone lines, organizations lose the added security that results from restricting physical access to computer terminal and other input devices. In such cases, the agency believes firms would be prudent to implement additional security measures above and beyond those controls that the organization would use if the access device was within its facility and commensurate with the potential consequences of such unauthorized access. Such additional controls might include, for example, use of input device checks, caller identification checks (phone caller identification), call backs, and security cards.

45. Proposed § 11.3(b)(5) defined electronic record as a document or writing comprised of any combination of text, graphic representation, data, audio information, or video information, that is created, modified, maintained, or transmitted in digital form by a computer or related system. Many comments suggested revising the proposed definition to reflect more accurately the nature of electronic records and how they differ from paper records. Some comments suggested distinguishing between machine readable records and paper records created by machine. Some comments noted that the term "document or writing" is inappropriate for electronic records because electronic records could be any combination of pieces of information assembled (sometimes on a transient basis) from many noncontiguous places, and because the term does not accurately describe such electronic information as raw data or voice mail. Two comments suggested that the agency adopt definitions of electronic record that were established, respectively, by the United Nations Commission on International Trade Law (UNCITRAL) Working Group on Electronic Data Interchange, and the American National Standards Institute/ Institute of Electrical and Electronic Engineers Software Engineering (ANSI/ IEEE) Standard (729–1983).

The agency agrees with the suggested revisions and has revised the definition of "electronic record" to emphasize this unique nature and to clarify that the agency does not regard a paper record to be an electronic record simply because it was created by a computer system. The agency has removed "document or writing" from this definition and elsewhere in part 11 for the sake of clarity, simplicity, and consistency.

However, the agency believes it is preferable to adapt or modify the words "document" and "writing" to electronic technologies rather than discard them entirely from the lexicon of computer technology. The agency is aware that the terms "document" and "electronic document" are used in contexts that clearly do not intend to describe paper. Therefore, the agency considers the terms "electronic record" and "electronic document" to be generally synonymous and may use the terms "writing," "electronic document," or "document" in other publications to describe records in electronic form. The agency believes that such usage is a prudent conservation of language and is consistent with the use of other terms and expressions that have roots in older technologies, but have nonetheless been adapted to newer technologies. Such terms include telephone "dialing," internal combustion engine "horse power," electric light luminance expressed as "foot candles," and (more relevant to computer technology) execution of a "carriage return."

Accordingly, the agency has revised the definition of electronic record to mean "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."

46. Proposed § 11.3(b)(6) defined an electronic signature as the entry in the form of a magnetic impulse or other form of computer data compilation of any symbol or series of symbols, executed, adopted or authorized by a person to be the legally binding equivalent of the person's handwritten signature. One comment supported the definition as proposed, noting its consistency with dictionary definitions (*Random House Dictionary of the English Language*, Unabridged Ed. 1983, and *American Heritage Dictionary*, 1982). Several other comments, however, suggested revisions. One comment suggested replacing "electronic signature" with "computer based signature," "authentication," or "computer based authentication" because "electronic signature" is imprecise and lacks clear and recognized meaning in the information security and legal professions. The comment suggested a definition closer to the UNCITRAL draft definition:

> (1) [a] method used to identify the originator of the data message and to indicate the originator's approval of the information contained therein; and (2) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all circumstances, including any agreement between the originator and the addressee of the data message.

One comment suggested replacing "electronic signature" with "electronic identification" or "electronic authorization" because the terms include many types of technologies that are not easily distinguishable and because the preamble to the proposed rule gave a rationale for using "electronic signature" that was too "esoteric for practical consideration."

The agency disagrees that "electronic signature" as proposed should be replaced with other terms and definitions. As noted in the preamble to the proposed rule, the agency believes that it is vital to retain the word "signature" to maintain the equivalence and significance of various electronic technologies with the traditional handwritten signature. By not using the word "signature," people may treat the electronic alternatives as less important, less binding, and less in need of controls to prevent falsification. The agency also believes that use of the word signature provides a logical bridge between paper and electronic technologies that facilitates the general transition from paper to electronic environments. The term helps people comply with current FDA regulations that specifically call for signatures. Nor does the agency agree that this reasoning is beyond the reach of practical consideration.

The agency declines to accept the suggested UNCITRAL definition because it is too narrow in context in that there is not always a specified message addressee for electronic records required by FDA regulations (e.g., a batch production record does not have a specific "addressee").

47. Concerning the proposed definition of "electronic signature," other comments suggested deletion of the term "magnetic impulse" to render the term media neutral and thus allow for such alternatives as an optical disk. Comments also suggested that the term "entry" was unclear and recommended its deletion. Two comments suggested revisions that would classify symbols as an electronic signature only when they are committed to permanent storage because not every computer entry is a signature and processing to permanent storage must occur to indicate completion of processing.

The agency advises that the proposal did not limit electronic signature recordings to "magnetic impulse" because the proposed definition added, "or other form of computer data * * *." However, in keeping with the agency's intent to accept a broad range of technologies, the terms "magnetic impulse" and "entry" have been removed from the proposed definition. The agency believes that recording of computer data to "permanent" storage is not a necessary or warranted qualifier because it is not relevant to the concept of equivalence to a handwritten signature. In addition, use of the qualifier regarding permanent storage could impede detection of falsified records if, for example, the signed falsified record was deleted after a predetermined period (thus, technically not recorded to "permanent" storage). An individual could disavow a signature because the record had ceased to exist.

For consistency with the proposed definition of handwritten signature, and to clarify that electronic signatures are those of individual human beings, and not those of organizations (as included in the act's definition of "person"), FDA is changing "person" to "individual" in the final rule.

Accordingly, § 11.3(b)(7) defines electronic signature as 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.

48. Proposed § 11.3(b)(7) (redesignated § 11.3(b)(8) in the final rule) defined "handwritten signature" as the name of an individual, handwritten in script by that individual, 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 proposed definition also stated that the scripted name, while conventionally applied to paper, may also be applied to other devices which capture the written name.

Many comments addressed this proposed definition. Two comments suggested that it be deleted on the grounds it is redundant and that, when handwritten signatures are recorded electronically, the result fits the definition of electronic signature.

The agency disagrees that the definition of handwritten signature should be deleted. In stating the criteria under which electronic signatures may be used in place of traditional handwritten signatures, the agency believes it is necessary to define handwritten signature. In addition, the agency believes that it is necessary to distinguish handwritten signatures from electronic signatures because, with handwritten signatures, the traditional act of signing one's name is preserved. Although the handwritten signature recorded electronically and electronic signatures, as defined in part 11, may both ultimately result in magnetic impulses or other forms of computerized symbol representations, the means of achieving those recordings and, more importantly, the controls needed to ensure their reliability and trustworthiness are quite different. In addition, the agency believes that a definition for handwritten signature is warranted to accommodate persons who wish to implement record systems that are combinations of paper and electronic technologies.

49. Several comments suggested replacing the reference to "scripted name" in the proposed definition of handwritten signature with "legal mark" so as to accommodate individuals who are physically unable to write their names in script. The comments asserted that the term "legal mark" would bring the definition to closer agreement with generally recognized legal interpretations of signature.

The agency agrees and has added the term "legal mark" to the definition of handwritten signature.

50. One comment recommended that the regulation state that, when the handwritten signature is not the result of the act of signing with a writing or marking instrument, but is applied to another device that captures the written name, a system should verify that the owner of the signature has authorized the use of the handwritten signature.

The agency declines to accept this comment because, if the act of signing or marking is not preserved, the type of signature would not be considered a handwritten signature. The comment appears to be referring to instances in which one person authorizes someone else to use his or her stamp or device. The agency views this as inappropriate when the signed record does not clearly show that the stamp owner did not actually execute the signature. As discussed elsewhere in this preamble, the agency believes that where one person authorizes another to sign a document on his or her behalf, the second person must sign his or her own name (not the name of the first person) along with some notation that, in doing so, he or she is acting in the capacity, or on behalf, of the first person.

51. One comment suggested that where handwritten signatures are captured by devices, there should be a register of manually written signatures to enable comparison for authenticity and the register also include the typed names of individuals.

The agency agrees that the practice of establishing a signature register has merit, but does not believe that it is necessary, in light of other part 11 controls. As noted elsewhere in this preamble (in the discussion of proposed § 11.50), the agency agrees that human readable displays of electronic records must display the name of the signer.

52. Several comments suggested various editorial changes to the proposed definition of handwritten signature including: (1) Changing the word "also" in the last sentence to "alternatively," (2) clarifying the

difference between the words "individual" and "person," (3) deleting the words "in a permanent form," and (4) changing "preserved" to "permitted." One comment asserted that the last sentence of the proposed definition was unnecessary.

The agency has revised the definition of handwritten signature to clarify its intent and to keep the regulation as flexible as possible. The agency believes that the last sentence of the proposed definition is needed to address devices that capture handwritten signatures. The agency is not adopting the suggestion that the word "preserved" be changed to "permitted" because "preserved" more accurately states the agency's intent and is a qualifier to help distinguish handwritten signatures from others. The agency advises that the word "individual" is used, rather than "person," because the act's definition of person extends beyond individual human beings to companies and partnerships. The agency has retained the term "permanent" to discourage the use of pencils, but recognizes that "permanent" does not mean eternal.

53. One comment asked whether a signature that is first handwritten and then captured electronically (e.g., by scanning) is an electronic signature or a handwritten signature, and asked how a handwritten signature captured electronically (e.g., by using a stylus-sensing pad device) that is affixed to a paper copy of an electronic record would be classified.

FDA advises that when the act of signing with a stylus, for example, is preserved, even when applied to an electronic device, the result is a handwritten signature. The subsequent printout of the signature on paper would not change the classification of the original method used to execute the signature.

54. One comment asserted that a handwritten signature recorded electronically should be considered to be an electronic signature, based on the medium used to capture the signature. The comment argued that the word signature should be limited to paper technology.

The agency disagrees and believes it is important to classify a signature as handwritten based upon the preserved action of signing with a stylus or other writing instrument.

55. One comment asked if the definition of handwritten signature encompasses handwritten initials.

The agency advises that, as revised, the definition of handwritten signature includes handwritten initials if the initials constitute the legal mark executed or adopted with the present intention to authenticate a writing in a permanent form, and where the method of recording such initials involves the act of writing with a pen or stylus.

56. Proposed § 11.3(b)(8) (redesignated as § 11.3(b)(9) in the final rule) defined an open system as an environment in which there is electronic communication among multiple persons, where system access extends to people who are not part of the organization that operates the system.

Several comments suggested that, for simplicity, the agency define "open system" as any system that does not meet the definition of a closed system. One comment suggested that the definition be deleted on the grounds it is redundant, and that it is the responsibility of individual firms to take appropriate steps to ensure the validity and security of applications and information, regardless of whether systems are open or closed. Other comments suggested definitions of "open system" that were opposite to what they suggested for a closed system.

The agency has revised the definition of open system to mean "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." The agency believes that, for clarity, the definition should stand on its own rather than as any system that is not closed. The agency rejects the suggestion that the term need not be defined at all because FDA believes that controls for open systems merit distinct provisions in part 11 and defining the term is basic to understanding which requirements apply to a given system. The agency agrees that companies have the responsibility to take steps to ensure the validity and security of their applications and information. However, FDA finds it necessary to establish part 11 as minimal requirements to help ensure that those steps are, in fact, acceptable.

VII. Electronic Records—Controls for Closed Systems (§ 11.10)

The introductory paragraph of proposed § 11.10 states that:

> Closed 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, and to ensure that the signer cannot readily repudiate the signed record as not genuine. * * *

The rest of the section lists specific procedures and controls.

57. One comment expressed full support for the list of proposed controls, calling them generally appropriate and stated that the agency is correctly accommodating the fluid nature of various electronic record and electronic signature technologies. Another comment, however, suggested that controls should not be implemented at the time electronic records are first created, but rather only after a document is accepted by a company.

The agency disagrees with this suggestion. To ignore such controls at a stage before official acceptance risks compromising the record. For example, if "preacceptance" records are signed by technical personnel, it is vital to ensure the integrity of their electronic signatures to prevent record alteration. The need for such integrity is no less important at preacceptance stages than at later stages when managers officially accept the records. The possibility exists that some might seek to disavow, or avoid FDA examination of, pertinent records by declaring they had not been formally "accepted." In addition, FDA routinely can and does inspect evolving paper documents (e.g., standard operating procedures and validation protocols) even though they have yet to receive a firm's final acceptance.

58. One comment said proposed § 11.10 contained insufficient requirements for firms to conduct periodic inspection and monitoring of their own systems and procedures to ensure compliance with the regulations. The comment also called for a clear identification of the personnel in a firm who would be responsible for system implementation, operation, change control, and monitoring.

The agency does not believe it is necessary at this time to codify a self-auditing requirement, as suggested by the comment. Rather, the agency intends to afford organizations flexibility in establishing their own internal mechanisms to ensure compliance with part 11. Self-audits, however, may be considered as a general control, within the context of the introductory paragraph of § 11.10. The agency encourages firms to conduct such audits periodically as part of an overall approach to ensure compliance with FDA regulations generally. Likewise, the agency does not believe it is necessary or practical to codify which individuals in an organization should be responsible for compliance with various provisions of part 11. However, ultimate responsibility for part 11 will generally rest with persons responsible for electronic record content, just as responsibility for compliance with paper record requirements generally lies with those responsible for the record's content.

59. Several comments interpreted proposed § 11.10 as applying all procedures and controls to closed systems and suggested revising it to permit firms to apply only those procedures and controls they deem necessary for their own operations, because some requirements are excessive in some cases.

The agency advises that, where a given procedure or control is not intended to apply in all cases, the language of the rule so indicates. Specifically, use of operational checks (§ 11.10(f)) and device checks (§ 11.10(h)) is not required in all cases. The remaining requirements do apply in all cases and are, in the agency's opinion, the minimum needed to ensure the trustworthiness and reliability of electronic record systems. In addition, certain controls that firms deem adequate for their routine internal operations might nonetheless leave records vulnerable to manipulation and, thus, may be incompatible with FDA's responsibility to protect public health. The suggested revision would effectively permit firms to implement various controls selectively and possibly shield records from FDA, employ unqualified personnel, or permit employees to evade responsibility for fraudulent use of their electronic signatures.

The agency believes that the controls in § 11.10 are vital, and notes that almost all of them were suggested by comments on the ANPRM. The agency believes the wording of the regulation nonetheless permits firms maximum flexibility in how to meet those requirements.

60. Two comments suggested that the word "confidentiality" in the introductory paragraph of proposed § 11.10 be deleted because it is unnecessary and inappropriate. The comments stated that firms should determine if certain records need to be confidential, and that as long as records could not be altered or deleted without appropriate authority, it would not matter whether they could read the records.

The agency agrees that not all records required by FDA need to be kept confidential within a closed system and has revised the reference in the introductory paragraph of § 11.10 to state "* * * and, when appropriate, the confidentiality of electronic records." The agency believes, however that the need for retaining the confidentiality of certain records is not diminished because viewers cannot change them. It may be prudent for persons to carefully assess the need for record confidentiality. (See, e.g., 21 CFR 1002.42, Confidentiality of records furnished by dealers and distributors, with respect to certain radiological health products.) In addition, FDA's obligation to retain the confidentiality of information it receives in some submissions hinges on the degree to which the submitter maintains confidentiality, even within its own organization. (See, e.g., 21 CFR 720.8(b) with respect to cosmetic ingredient information in voluntary filings of cosmetic product ingredient and cosmetic raw material composition statements.)

61. One comment asked if the procedures and controls required by proposed § 11.10 were to be built into software or if they could exist in written form.

The agency expects that, by their nature, some procedures and controls, such as use of time-stamped audit trails and operational checks, will be built into hardware and software. Others, such as validation and determination of personnel qualifications, may be implemented in any appropriate manner regardless of whether the mechanisms are driven by, or are external to, software or hardware. To clarify this intent, the agency has revised the introductory paragraph of proposed § 11.10 to read, in part, "Persons who use closed systems to create, modify * * *." Likewise, for clarity and consistency, the agency is introducing the same phrase, "persons who use * * *" in §§ 11.30 and 11.300.

62. One comment contended that the distinction between open and closed systems should not be predominant because a $100,000 transaction in a closed system should not have fewer controls than a $1 transaction in an open system.

The agency believes that, within part 11, firms have the flexibility they need to adjust the extent and stringency of controls based on any factors they choose, including the economic value of the transaction. The agency does not believe it is necessary to modify part 11 at this time so as to add economic criteria.

63. One comment suggested that the reference to repudiation in the introductory paragraph of § 11.10 should be deleted because repudiation can occur at any time in legal proceedings. Another comment, noting that the proposed rule appeared to address only nonrepudiation of a signer, said the rule should address nonrepudiation of record "genuineness" or extend to nonrepudiation of submission, delivery, and receipt. The comment stated that some firms provide nonrepudiation services that can prevent someone from successfully claiming that a record has been altered.

In response to the first comment, the agency does not agree that the reference to repudiation should be deleted because reducing the likelihood that someone can readily repudiate an electronic signature as not his or her own, or that the signed record had been altered, is vital to the agency's basic acceptance of electronic signatures. The agency is aware that the need to deter such repudiation has been addressed in many forums and publications that discuss electronic signatures. Absent adequate controls, FDA believes some people would be more likely to repudiate an electronically-signed record because of the relative ease with which electronic records may be altered and the ease with which one individual could impersonate another. The agency notes, however, that the rule does not call for nonrepudiation as an absolute guarantee, but requires that the signer cannot "readily" repudiate the signature.

In response to the second comment, the agency agrees that it is also important to establish nonrepudiation of submission, delivery, and receipt of electronic records, but advises that, for purposes of § 11.10, the agency's intent is to limit nonrepudiation to the genuineness of the signer's record. In other words, an individual should not be able to readily say that: (1) He or she did not, in fact, sign the record; (2) a given electronic record containing the individual's signature was not, in fact, the record that the person signed; or (3) the originally signed electronic record had been altered after having been signed.

64. Proposed § 11.10(a) states that controls for closed systems are to include the validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to conclusively discern invalid or altered records.

Many comments objected to this proposed requirement because the word "conclusively" inferred an unreasonably high and unattainable standard, one which is not applied to paper records.

The agency intends to apply the same validation concepts and standards to electronic record and electronic signature systems as it does to paper systems. As such, FDA does not intend the word "conclusively" to suggest an unattainable absolute and has, therefore, deleted the word from the final rule.

65. One comment suggested qualifying the proposed validation requirement in § 11.10(a) to state that validation be performed "where