59 Federal Register 45160, 8/31/94

DEPARTMENT OF HEALTH AND HUMAN SERVICES
FOOD AND DRUG ADMINISTRATION
21 CFR PART 11

[DOCKET NO. 92N-0251]
ELECTRONIC SIGNATURES; ELECTRONIC RECORDS

AGENCY: Food and Drug Administration, HHS.

ACTION: Proposed rule.

SUMMARY: The Food and Drug Administration (FDA) is proposing regulations that would, under certain circumstances, permit the agency to accept electronic records, electronic signatures, and handwritten signatures executed to electronic records as generally equivalent to paper records and handwritten signatures executed on paper. These proposed regulations would apply to records when submitted in electronic form that are called for in Title 21 of the Code of Federal Regulations (CFR). The use of electronic forms of recordkeeping and submissions to FDA remains voluntary. This proposed rule is a followup to the agency's July 21, 1992, advance notice of proposed rulemaking (ANPRM). The intended effect of this proposed rule is to permit use of electronic technologies in a manner that is consistent with FDA's overall mission and that preserves the integrity of the agency's enforcement activities. This proposed rule is also intended to assist in achieving the objectives of the Vice President's National Performance Review.

DATES: Written comments by November 29, 1994. FDA proposes that any final rule based on this proposal be effective 90 days after its publication in the FEDERAL REGISTER.

ADDRESSES: Submit written comments to the Dockets Management Branch (HFA-305), Food and Drug Administration, rm. 1-23, 12420 Parklawn Dr., Rockville, MD 20857.

FDA encourages interested persons who elect to send their comments by e-mail to also send two paper copies of their comments to the Dockets Management Branch (address above). The INTERNET (92N0251@A1.FDAOC.FDA.GOV) address is only for this docket and will be disabled after the comment period closes. However, based upon the outcome of this proposed rule, FDA may extend acceptance of comments by e-mail to other dockets in the future.

This proposed rule is available via INTERNET and BITNET by sending an e-mail

message to DOC00001@FDACD.BITNET. The sole purpose of this electronic address is to automatically distribute the proposed rule by return e-mail. Therefore, no other correspondence should be sent to this electronic address, and there is no need to include text in the body or subject of the electronic request message. However, to permit any necessary followup, persons may include their names, postal addresses, and phone numbers in the body of the messages.

FOR FURTHER INFORMATION CONTACT:

Paul J. Motise,
Center for Drug Evaluation and Research (HFD-323),
Food and Drug Administration,
7520 Standish Pl.,
Rockville, MD 20855,
301-594-1089.
E-mail address via MCI Mail:
Name: Paul J. Motise, EMS: FDA, MBX: MOTISE, MBX: A1, MBX: FDACD.
(For help in addressing format contact the MCI Mail Customer Support Line (1-800-444-6245)); or
Tom M. Chin,
Division of Compliance Policy (HFC-230),
Food and Drug Administration,
5600 Fishers Lane,
Rockville, MD 20857,
301-443-1500.

SUPPLEMENTARY INFORMATION:

I. BACKGROUND

In the FEDERAL REGISTER of July 21, 1992 (57 FR 32185), FDA published an ANPRM on whether the agency should propose regulations that would, under certain circumstances, permit the agency to accept electronic identification or electronic signatures in place of handwritten signatures where signatures are required in 21 CFR, and where the electronic form of the signature bearing record is allowable by the regulations. The ANPRM requested comments on current and future electronic records maintained by industry and subject to FDA inspection, submitted to FDA for review and approval, and FDA's own records and industry notifications. The ANPRM also identified and sought specific comment on the following issues: (1) Regulatory acceptance; (2) enforcement integrity; (3) security; (4) validation; (5) standards; and (6) freedom of information (FOI). In the FEDERAL REGISTER of October 21, 1992 (57 FR 48008), FDA published an extension of the comment period regarding the ANPRM. Interested persons were given until December 18, 1992, to comment on the ANPRM.

FDA received 53 comments from trade associations, pharmaceutical and medical device manufacturers, computer systems developers, private organizations, a Federal agency, a university, and consumers. The comments generally support the ANPRM's objectives. A number of the comments made suggestions. As appropriate, comments will be responded to in this document in the discussion of the proposed regulation set forth below.

II. SUMMARY AND ANALYSIS OF COMMENTS TO THE ANPRM

A. Analysis of Comments

The agency received a total of 53 comments to the July 21, 1992, ANPRM. Comments came from a variety of sources including: 6 trade associations, 27 pharmaceutical manufacturers, 2 medical device manufacturers, 1 contract laboratory, 8 computer systems developers, 1 law firm on behalf of a computer systems developer, 1 law firm on behalf of a consortium of industrial research companies, 1 agency of the Federal Government, 1 drug sample distribution establishment, one medical center, 1 university food sciences unit, 1 express mail delivery service, and 2 individuals.

Comments generally supported the agency's efforts relative to electronic signatures and electronic records. One comment suggested that FDA's actions may provide a model for other Federal agencies. Several comments found the agency's electronic identification issues to be among the most important and immediate concerns currently facing the pharmaceutical industry. One comment expressed concern that the ANPRM did not address medical devices and urged the agency to adopt uniform agency-wide policies regarding electronic signatures.

In general, comments addressed the advantages of electronic records in enhancing product quality, control, production efficiency, and the conduct of nonclinical laboratory studies. Comments urged the agency to follow a course of action that would not impede technological innovation. Comments also called for expedited resolution of the issues in order to facilitate industry's plans for implementing new technologies.

One comment commended the agency for making the February 24, 1992, progress report of the FDA Electronic Identification/ Signature Working Group available via e-mail and encouraged FDA to continue electronic distribution of agency documents. One comment submitted a 58-page paper which addressed legal considerations and a detailed stratification scheme based upon security risks.

Although the ANPRM stated that the scope of FDA's considerations extends to all articles that it regulates, and to all portions of 21 CFR under its jurisdiction, very few comments were received from sources outside the pharmaceutical industry. One medical device trade association mistakenly commented that medical devices were not covered. The agency emphasizes that all regulated articles are covered. The agency agrees that it is important to accommodate new technologies in a responsible manner. The agency also agrees with the comment that encouraged FDA to continue electronic

distribution of agency documents. FDA will be implementing this form of distribution increasingly in the future.

The decision to propose these rules is based upon: (1) The information and comments submitted in response to the July 21, 1992, ANPRM; (2) the recommendations and findings of the agency's Task Force on Electronic Identification/Signatures, which was reported in the progress report of FDA's Electronic Identification/Signature Working Group on February 24, 1992 (Ref. 1); and (3) the agency's experience with alternatives to conventional handwritten signatures and electronic records. The agency is aware that automated systems are being used more extensively in the various industries that it regulates. Use of such systems is also expanding within the agency itself. Implementing paperless electronic records and attendant methods of "signing" such records is an emerging objective of the use of automation. Signatures are a key aspect of many records. The transition from paper records containing traditional handwritten signatures to paperless electronic records raises issues relating to FDA's acceptance of alternatives to handwritten signatures and their underlying trustworthiness.

FDA recognizes the importance of electronic records and their integration into a variety of automation efforts, such as manufacturing process controls, materials resources controls, laboratory information systems, clinical trial information systems, and electronic data interchange activities. The agency is aware that some new technologies and manufacturing methods require use of electronic records. For example, in certain highly controlled manufacturing environments, the presence of paper itself can pose a source of product contamination, and (for highly toxic compounds) paper can be a vehicle for exposing workers to dangerous compounds.

FDA is aware of the benefits of conducting official electronic communication with regulated industries and the public. However, the agency is also aware that legal, regulatory, and administrative concerns have delayed full use of electronic communication. FDA expects that promulgation of the regulations proposed in this document will begin to address the agency's concerns and facilitate the agency's modernization efforts.

Although most comments to the ANPRM addressed electronic records within the context of closed systems, where access is limited to people who are part of the organization that operates the system, the agency expects that near-term development and implementation of appropriate controls for open systems, where access extends to people outside of the operating organization, will facilitate secure, authoritative electronic communication between FDA and the regulated industries.

The Vice President's Report of the National Performance Review has as a stated objective the expanded use of new technologies and telecommunications to create an "electronic government." (September 7, 1993, Report of the Vice President's National Performance Review (pp. 113 through 117) (Ref. 2)). This proposal would be a first step by FDA in implementing this objective, by, for example, allowing electronic filings of regulatory documents and expanded use of e-mail. This will result in significant benefits to the public, the regulated industry, and the agency. These benefits could

include faster review and approval of new products, and rapid availability of a variety of agency documents around the clock.

FDA encourages the use of new technologies that will enhance the quality, safety, and efficacy of products it regulates, but is mindful of the need to maintain the ability to fulfill its consumer protection mandate. The agency believes that these proposed rules will accomplish both objectives.

B. Comments on Record Types

The ANPRM requested examples of records that: (1) Are maintained by industry and inspected by FDA, (2) are submitted to FDA, and (3) are created and maintained by FDA that may be amenable to electronic identification/signatures. Most respondents confined their comments to the first record type. However, a few comments provided the following examples of records in each category:

Records maintained by industry and inspected by FDA that may be in electronic form include:

1. Master and batch production and control records,
2. Logs,
3. Standard operating procedures,
4. Laboratory notebooks,
5. Complaint records,
6. Validation protocols and data summaries,
7. Laboratory data summaries, and
8. Drug sample records under the Prescription Drug Marketing Act (the PDMA) (Pub. L. 102-353).

Although most comments addressed pharmaceutical records, the agency believes that it is necessary to recognize that records maintained by industry and inspected by FDA extend to other articles and include records such as:

1. Medical device history records, and medical device master records,
2. Master record files,
3. Blood bank donor records,
4. Thermally processed low-acid foods records, and
5. Hazard analysis critical control points

Records submitted to FDA that may be in electronic form include:

1. New drug or new animal drug applications,
2. Product license applications,
3. Establishment license applications, and
4. Drug or veterinary drug master files.

Most comments focused on pharmaceutical documents. However, the agency recognizes that submissions for other FDA-regulated products would be applicable. Such records include, but are not limited to:

1. Medical device premarket approval applications,
2. Medical device premarket notifications,

3. Medicated feed applications,
4. Food additive petitions,
5. Color additive petitions,
6. Infant formula notifications,
7. Low acid canned food and acidified food firm, registration and scheduled process filing, and
8. Generally recognized as safe (GRAS) petitions.

One comment addressed records maintained by the agency and suggested that signatures recorded electronically (SRE's), as identified in the ANPRM, should be an acceptable alternative to signatures recorded on paper. The comment asserted that SRE's have sufficient uniqueness, are difficult to forge (especially when accompanied by the date and time the SRE was made), and would realize legal acceptance.

Two comments suggested that whatever policies are adopted for electronic records maintained by the industry, or records submitted to the agency, apply equally to FDA's own records. Although the proposed rule focuses primarily on records maintained by industries inspected by FDA, and submissions to the agency, FDA will apply the principles in the new rule to its own electronic documents.

III. DEFINITIONS/STRATIFIED ACCEPTANCE APPROACH

A. Definitions

One comment agreed with FDA's working definitions. The comment noted that electronic identification should suffice for all of the agency's applications and called for common codified definitions for the following words and phrases.

1. Signature

Several comments agreed with FDA's working definition of the term "signature." One categorized conventional signatures as "wet signatures" and one submission suggested renaming the term "handwritten signatures" for clarification.

2. Signatures Recorded Electronically

One comment suggested that the term "signatures recorded electronically" be defined as an electronically captured image of a handwritten signature on optical, magnetic or other electronic media. One comment agreed with the working definition.

3. Electronic Signature

Several comments called the working definition of the term "electronic signature" as acceptable and useful. However, some comments claimed that the term is imprecise and potentially confusing to the extent that the word "signature" also appears in other working definitions. Several comments suggested the alternative phrases: "Biometric/behavioral identification" and "biologically-based electronic identification."

One comment referred to its security code number assignment system as an electronic signature, used by physicians to phone in requests for additional drug samples previously reserved under the physicians' names. Telephone requests are followed up by confirmatory signed paper forms.

4. Electronic Identification

Many comments suggested that FDA define only two terms, "signatures" (meaning conventional handwritten signatures) and "electronic identification" (to encompass signatures recorded electronically, electronic signatures, and all other forms of electronic identification). Comments suggested that definitions should not imply superiority of one type of endorsement over another and offered the following definition of electronic identification: "any method for identifying an individual where the act of providing a personal mark (signing) is recognized and/or recorded electronically."

Comments asserted that secure, validated computer systems that use electronic identification provide better, or at least equivalent, authentication than systems using handwritten signatures.

One comment suggested that a more precise term would be "administratively controlled electronic identification." One comment said that its digital signature encryption technology, a system using encrypted "keys" and proprietary algorithms, would meet the agency's working definition of electronic identification, but could be coupled with hardware and software that utilize biometric links to meet the definition of electronic signature.

5. Other Definitions

Two comments offered the following additional defined terms: "Signature Alternative"--an electronically recorded mark from any type of electronic identification, not involving a signature recorded electronically, including electronic signature (biometric/behavioral identification) and, administratively controlled electronic identification.

"Signing"--the act of providing a personal recorded mark that serves as identification. The mark can be, but is not necessarily, provided by handwriting. The mark may also be provided by a stamp, seal, or electronic device. The last example typically records the mark in magnetic or optical media rather than on paper.

The agency believes that the diversity of comments on definitions reflects the variety of signature technologies that are available, and the need for a simple codified definition of as few terms as possible. The agency is persuaded by the general premise, expressed in many comments, that FDA should establish only two definitions based broadly on whether or not the "signature" is handwritten. Therefore, the agency is proposing to codify two definitions, one for "handwritten signature" and one for "electronic signature." Electronic signature would include electronic identification; handwritten signatures would include signatures recorded electronically.

FDA disagrees with the assertion that "electronic identification," rather than "electronic signature" should be one of the two broad terms, for several reasons. The agency believes the appearance of the word "signature" in both "electronic signature" and "handwritten signature" will not be confusing to the average person, especially where the codified definitions are clear.

More importantly, the agency believes that there are overriding advantages to maintaining the word "signature" in the term "electronic signature." The legal,

regulatory, and psychological importance that the average person has come to associate with conventionally signing a paper document is more likely to be carried over and equally applied to technological alternatives if the word signature is preserved. On the other hand, substitution of the word "identification" for "signature" may, on its face, imply that the alternative is something quite different and perhaps less significant. Thus, terminology can help to establish the functional equivalency of different technologies.

In addition, the term "electronic identification" can be too limiting in scope because signatures do more than merely identify the person who signed something that could be done by a person who did not perform the action. However, retention of the word "signature" in the term "electronic signature" conveys by direct inference all of the purposes of a handwritten signature, including identification, authentication, and affirmation. Accordingly, FDA is proposing in § 11.3 to define "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. However, the scripted name, while conventionally applied to paper, may also be applied to other devices which capture the written name.

"Electronic Signature" is defined in proposed § 11.3 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.

B. Biometric/Behavioral Links as Part of the Electronic Signature

Systems which utilize biometric/behavioral links as part of the electronic signature verify a person's identity based on measurement of an individual's physical feature(s) or repeatable action.

One comment addressed the behavioral link incorporated in a software product designed for use in pen-based computers; it described how the system provides reliability and trustworthiness by calibrating and recognizing a set of characteristics attendant to the act of signing (pen strokes, speed, acceleration, etc.). One comment provided a paper in support of a signature verification system that characterizes the act of signing to establish a behavioral link between the signer and the signature, noting the system's low error rate (0.19 percent false rejects and 0.56 percent false accepts), security, social acceptance, performance, low cost, and computer portability. The paper describes how the system could be used on networks or over phone lines, in conjunction with a microprocessor-based encryption card, to prevent transmission of a prerecorded (and possibly false) signature by requiring the generation of a signature for each endorsement.

One submission asserted that stable technologies exist to provide reliable and repeatable electronic verification of individuals based upon a biometric/behavioral link.

The comment furnished a report summarizing testing on several such systems that use fingerprints, hand geometry, the act of signing, retinal scans and voiceprints; the comment cited access control as the primary type of application for such systems.

Several comments argued against technologies that incorporate biometric/behavioral links on the grounds of excessive cost; two comments said biometric based devices cost about $1,800 to $4,000 per unit and behavioral based devices cost $600 to $1,500 each.

Most comments argued against the premise that biometric/behavioral links are necessary or beneficial to electronic signatures. However, two comments asserted that appropriate application of electronic signatures requires a biometric or direct behavioral link to an individual, and one comment acknowledged that such links are less susceptible to procedural deviations than other authentication methods. One comment said biometric/behavioral links are appropriate to systems which control physical access to a facility.

Many comments urged FDA to refrain from requiring use of systems based on biometric/behavioral links (particularly where the drug current good manufacturing practice (CGMP) regulations require signatures) on the grounds that:

1. Such a requirement would be contrary to the objectives of the CGMP regulations;
2. Electronic signature systems are not routinely used in non-FDA regulated industry;
3. Electronic signature technology is relatively immature and unreliable;
4. The technology is relatively expensive; and
5. Electronic signature devices are impractical for pharmaceutical applications in which operators are garbed so as to obscure anatomical interaction with detection devices (e.g., hand or voiceprints would be difficult to manage where workers wear masks or gloves).

FDA believes it is important to allow firms to take advantage of a variety of new technologies. It is not the agency's intent to mandate use of systems that use biometric/behavioral links, although the agency recognizes the potential advantages of such systems and encourages their development and adoption. Comments generally indicate that biometric/behavioral link technologies have been developed, may have high levels of reliability, but have not yet been incorporated into manufacturing environments to any appreciable degree. Accordingly, the agency's proposed regulations do not, at this time, specify the type of electronic signature technologies that are required.

However, because FDA recognizes the benefits of those electronic signatures which are inherently less vulnerable to falsification, and because the agency wishes to encourage the development of such technologies, the proposed regulations reflect the position that the robustness of biometric/behavioral based systems permits less stringent administrative controls to be used.

In addition, FDA considers that biometric/behavioral based systems may have greater application in open environments, which pose a greater challenge to signature

integrity than closed environments.

C. Purpose of Signatures

One comment identified the following functions of a signature: To identify someone; to declare, to witness, to acknowledge or disclaim, to agree or disagree, and to exhibit responsibility or authorship, as a formalized personal act such that subsequent disavowal or disclaimer is highly unlikely. The comment added that good practice suggests that the signature be properly ascertained, clearly indicated, and appropriately exhibited in a prominent place, and that bilateral mechanisms can further this purpose, and focus the individual's attention on the gravity, solemnity, and formality of the event. The comment also noted that because the purpose of a signature is not always apparent, some documents include clarifying phrases such as "in witness thereof," or "agreed to by." The comment further stated that in the typical manufacturing environment custom governs the meaning of a signature (e.g., to acknowledge performance of a procedure, responsibility for proper performance of the procedure, or to show that the person was merely present). The agency believes the comment has identified an important aspect of a signed writing, namely the meaning ascribed to the signature. Accordingly, the regulations proposed at § 11.50(b) require the document being signed to clearly indicate the purpose of the electronic signature. FDA also agrees with the comment's view that bilateral mechanisms can help to establish the seriousness of the electronic endorsement, and the agency is proposing at § 11.200(a)(1) to require certain electronic signatures to be composed of at least two elements.

Respondents also commented on how signature alternatives might fulfill the following traditional purposes of a signature:

1. To identify the actor and show his/her authority to act. Many comments disagreed that presence of a signature shows the signer's authority to act, noting that such authority is generally determined by the individual's organization. However, several comments acknowledged that electronic identification systems can be programmed to confirm an individual's authority to act.

One comment said authority to act could be met by the use of identification codes/passwords for intra-establishment records and by public key encryption standards such as the Rivest-Shamir- Adleman (RSA) standard for inter-establishment records.

The agency agrees that the presence of a signature, per se, does not necessarily guarantee that the signer has the authority indicated. However, in general, the presence of the signature, in combination with the signer's title, is by custom a reasonable indication that the person does have the organization's authority to endorse the subject document. FDA believes that in most cases people will not sign a document if they lack the authority called for by the action of signing. In the kinds of electronic environments addressed by the comments, systems can check a cross-referenced authorization roster to see that an individual who attempts to sign a

document has, in fact, the requisite authority.

2. To document the action in a way that is legally binding and cannot be repudiated.

Comments generally asserted that properly validated and secure electronic identification systems would be legally binding.

The agency agrees with the comments regarding the importance of validation and security and the proposed rule places appropriate emphasis on these controls.

One comment suggested that documentation of the action, not the individual, should be of prime importance because FDA is concerned more with the actions of a company than with individuals within a company, and that concern with actions of individuals is the concern of the company itself. The comment added that the RSA encryption standard could be used in this area for inter-establishment electronic records.

FDA disagrees with the premise that FDA should be concerned more with corporate than individual actions. In FDA's enforcement activities, there is equal emphasis on the responsibility of both individuals and corporations. Furthermore, section 201(e) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321(e)) defines a person to include an individual, partnership, corporation, and association.

3. To create a record that would be admissible in court. One comment suggested that a record should be admissible in court if it is shown that the record was generated by the responsible company, regardless of whether or not the record was signed; the RSA encryption standard was again cited as applicable for inter-establishment records. One submission said that electronic records would be admissible when authenticated by appropriate corporate officials under appropriate procedures relative to electronic identification.

The agency has found that court acceptance of records generally hinges on their reliability and trustworthiness. Although FDA agrees that a given unsigned record may be strictly admissible in a proceeding, establishing reliability and trustworthiness may well require that specific documents bear signatures of responsible individuals. In addition, as stated above, it is frequently important for FDA to establish individual, as well as corporate responsibility in pursuing regulatory actions, thus making it vital that evidentiary documents are signed by key individuals. The weight given to a piece of evidence may also depend upon the presence or absence of a verifiable signature.

D. Stratification

The ANPRM suggested that FDA might stratify acceptance of signature alternatives based upon the regulatory significance of the electronic record. Comments generally held that regulatory significance should not be the basis of stratification. Two comments argued against any regulatory stratification at all, one asserting that because conventional signatures are accepted in all situations, any alternative that provides security, identity, legibility and enforceability equal to or better than a handwritten signature should, likewise, be accepted for any application.

Two comments agreed with the concept of developing a stratified system whereby the regulatory significance of a record would determine the level of security needed for the signature alternative, but indicated that companies should individually define the various security categories and develop appropriate security procedures.

One comment said that electronic authorizations of high importance might require use of secondary passwords or codes to further augment security and verify data integrity.

Although most comments disagreed with the stratification approach suggested in the ANPRM, many comments suggested stratification along other lines, as follows:

1. Open Versus Closed Systems

Many comments suggested that stratification of signature alternatives be limited to security measures applied to inter versus intra company records. The distinction was stated in terms of "closed," versus "open" environments. Comments said that closed systems are typical in the pharmaceutical industry, and include administrative and physical controls to enhance reliability of the electronic endorsements.

Several comments described a typical CGMP closed system as: (1) Having controlled physical access; (2) having professionally written and approved procedures with employees and supervisors trained to follow them; (3) having records systems designed to facilitate quality assurance investigations when abnormalities may have occurred; and (4) being under legal obligation to the organization responsible for operating the system.

The following examples of documents in closed systems were given: CGMP records, GLP (good laboratory practice) and GCP (good clinical practice) records including clinical case reports, such submissions to FDA as new drug applications and adverse experience reports, and FDA internal records.

Comments generally characterized open systems as: (1) Having potentially greater exposure by outsiders; (2) entailing communication among multiple parties (e.g., communication by modem); and (3) extending system access to people who are not legally obligated to system managers.

Comments gave examples of open system documents including: Requests for drug samples, institutional review board (IRB) reviews of clinical protocols, GLP records, and Freedom of Information submissions to FDA.

2. Security Baseline Stratification for Open Systems

One comment presented a paper which addresses security stratification parameters based upon the risks of disclosure, where electronic messages are communicated in an "open" system. Stratification involves three security baselines, each of which considers the following message attributes: (1) Content sensitivity; (2) monetary value; (3) time sensitivity; (4) statutory security mandates; and (5) authentication certification requirements.

Message attributes, under the baseline system, determine the necessity and extent of the following security and reliability measures: (1) Noncryptographic identification and authentication; (2) systems controls to ensure authenticity, integrity, and

availability; (3) audit trails; (4) message authentication codes (MAC's); (5) digital signatures/encryption; and (6) electronic notarization.

Message attributes combined with appropriate security and reliability measures then determine the electronic document's legal effect: The degree to which the documents are considered to be legal signed writings that are authentic and enforceable to the same extent as comparable documents prepared using conventional paper-based mechanisms.

The agency has carefully considered the divergent comments on acceptance stratification and is persuaded that the regulatory significance of a document need not be the basis of such stratification. However, the comments reflected a general premise that the nature and extent of security measures necessary to reasonably establish the reliability, authenticity, and confidentiality of an electronic signed writing will vary to the extent that the writings are vulnerable to unauthorized alteration or loss.

The agency agrees with comments that a fundamental two tier stratification based upon open and closed systems, as comments described, is warranted. FDA anticipates that most electronic documents which are maintained by industry and inspected by the agency would be considered as falling within "closed" systems. Electronic records that are submitted to the agency, however, as indicated by the comments, may be considered to be within either "closed" or "open" systems depending on how they are delivered (i.e., via "open" e-mail, or "closed" hand-delivery by submitters or postal services). Likewise, FDA's own electronic records may be stratified as existing in either open or closed systems depending on how they are originated and, for certain records, transmitted to correspondents.

The proposed regulations place primary emphasis on electronic records in closed systems, because that approach would cover most of the emerging electronic records and would respond to the most urgent of industry's needs in developing electronic record systems. FDA considers "open" systems to be nonetheless important because correspondence and regulatory submissions conveyed by public electronic networks are gaining wider implementation. Therefore, FDA may, in the future, propose more specific requirements relating to open systems, as the agency gains additional information and experience with open systems and the controls that may be necessary to maintain the integrity and authenticity of electronic documents in that environment.

IV. LEGAL ACCEPTANCE

Several comments said that electronic records would, in fact, be admissible in court, provided that there are controls in place to make the records reasonably reliable and trustworthy. One comment cited several recent court cases in support of this acceptability.

The agency notes that although the ANPRM did not specifically request comments on legal acceptability of electronic records and signatures, the gist of most of the comments is that legal acceptance will not be hindered, provided that the records are shown to be reliable and trustworthy. The case transcript cited by the comment

included testimony from computer system operators which outlined key good computing practices that many of the comments also identified.

V. REGULATORY ACCEPTANCE

A. General Considerations

One comment suggested that the disparity among FDA regulations regarding acceptance of signature alternatives was based upon definitions that are either too weak or restrictive, and called for common regulatory definitions.

The agency believes that any regulatory disparity derives from a number of factors, including the degree to which various regulations anticipate use of electronic records in place of paper records, and specific program needs of different FDA centers. FDA believes that differences can be dispelled by promulgation of these uniform broad based regulations on electronic records/signatures. The agency agrees that common definitions in such regulations would help to harmonize policy across different parts of FDA.

One comment recommended that FDA issue a broad policy statement or inspectional guideline that would broadly accept electronic identification/signatures and that would at least establish criteria for the degree of security required for electronic identification/signature systems. The comment urged that no new regulations be issued.

The agency has determined that a policy statement, inspectional guide, or other guideline would be an inappropriate vehicle for accepting electronic signatures because such documents do not have the same legal significance as substantive regulations that require signatures. Guidance documents may be appropriate, however, to elaborate upon acceptance regulations.

B. Program Areas

1. Drug CGMP Regulations

Although the ANPRM applied to all FDA regulations in 21 CFR, most comments focused primarily on the CGMP regulations for drugs (parts 210 and 211 (21 CFR parts 210 and 211)). Some comments suggested that resolution of the issues in the CGMP context could be applied to resolve similar issues in the context of other FDA regulations.

Many comments argued that the existing CGMP regulations permit the use of electronic identification wherever documents are required to be signed, initialed, endorsed or approved, with the singular exception of § 211.186 (master production and control records) which explicitly requires full handwritten signatures. Comments supported their assertions by citing preamble comment paragraphs 186, 282, and 447 in the final rule on CGMP's in the FEDERAL REGISTER of September 29, 1978 (43 FR 45014), FDA's Compliance Policy Guide (CPG) 7132a.08, and (unspecified) tacit acceptance by FDA field investigators who encounter electronic identification.

One comment identified several sections of the CGMP regulations as requiring signatures, including § 211.188(b)(11) (batch production and control records), even though the word signature, per se, does not appear ("Identification of the persons performing and directly supervising or checking each significant step in the operation").

Comments urged the agency to issue a policy statement (such as a CPG), in the near term, that would condone use of electronic identification for all applications of signatures in the regulations, except § 211.186. Comments requested that in the long term, § 211.186 be amended to delete reference to handwritten signatures and accept electronic identification. The agency does not agree with the assertions that, except for § 211.186, the CGMP regulations currently permit alternatives to handwritten signatures or initials. (See findings of the Electronic Identification/Signatures Working Group in its February 24, 1992, progress report.) The Center for Drug Evaluation and Research, in consultation with the Office of the General Counsel, considered and rejected as inappropriate the issuance of a CPG that would accept "electronic identification" or other signature alternatives, even before the working group was formed.

The agency's conclusion regarding what the CGMP's allow was conveyed to the Pharmaceutical Manufacturers Association in a letter of December 5, 1991 (Ref. 3). Furthermore, the compliance policy guide cited by comments is not directly relevant because it addresses second check endorsements for operations executed by machine, rather than the form that human endorsements take. In addition, although comments cite several paragraphs of the 1978 FEDERAL REGISTER notice as supportive of their assertions, they overlook a key paragraph in which the agency clearly rejected substitution of employee numbers or codes for signatures or initials, on the basis of psychological differences from the act of signing and because of ease of falsification (43 FR 45068, September 29, 1978 (comment 433)).

The agency advises that some sections of the CGMP regulations, while not using the words sign, signature, or initials, nonetheless implicitly require endorsements to be in the form of handwritten signatures or initials. For example, the provisions of § 211.188 require batch production and control records to contain the "[i]dentification of the persons performing and directly supervising or checking each significant step in the operation." FDA investigators have historically encountered and expect to find the identification to take the form of a signature. Some developers of automation systems also recognize that "identification" means "signature."

Accordingly, the agency is not issuing the suggested CPG, but is, instead, proposing these acceptance regulations, that would cover records required by most FDA regulations, including the CGMP regulations. However, the agency may issue clarifying guidance documents, as needed, after such regulations are in effect.

2. Regulatory Submissions

Two comments said that regulations that require signatures on new drug applications necessitate substantial additional handling to furnish paper based

signatures where the basic submissions are in electronic form. Comments suggested that the agency require submissions to contain, in lieu of the additional paper, a statement that signatures (handwritten or otherwise) are "on file." The comment added that FDA could verify those endorsements during its inspections. The comments observed further that when electronic submissions are copied or converted among various computer file formats, electronic endorsements might be omitted.

One comment stated that resolution of issues associated with electronic identification and the transfer or conversion of electronic data will be necessary if the benefits of electronic submissions are to be achieved.

The agency believes that codified acceptance of electronic signatures in lieu of handwritten signatures will address the issues relating to regulatory submissions. Acceptance of electronic signatures would, in most cases, obviate the need to have paper based handwritten signatures on file as a reference. However, the agency notes, from the comments, the importance of having the electronic records include the printed name of the signer so as to clearly identify the signer.

3. Prescription Drug Marketing Act

Several comments cited the signature requirements (for requesting and receiving samples of prescription drugs) in the PDMA provisions of the Federal Food, Drug, and Cosmetic Act, and based on the increasing use of computer technology to transact the handling of such requests, urged the agency to accept electronic identification in lieu of handwritten paper based signatures. Another comment echoed the same suggestion, recommending that biometric/behavioral links not be required, but noting also that physician requests for drug samples are generally made in "open" environments such that use of certain alternatives for full electronic or handwritten signatures needs review.

One comment requested that, for purposes of the PDMA, FDA accept SRE's based upon their uniqueness and reliability, and that such acceptance be codified in regulations. Another comment described its SRE pen-computer based system, emphasizing the nonalterability of signed electronic records to merit regulatory acceptance.

One comment assumed that the ANPRM did not pertain to the PDMA.

One comment asked that FDA issue implementing regulations under the PDMA that accept electronic signatures and that such issuance not be delayed pending the agency's broader consideration of electronic records and endorsements.

The proposed rule to implement certain parts of the PDMA and the Prescription Drug Amendments of 1992 was published in the FEDERAL REGISTER of March 14, 1994 (59 FR 11842). That proposed rule would prohibit the imprinting or automatic reproduction of a signature by a device or machine such as a stamp, copier, or autopen at 21 CFR 203.61(a). The agency recognizes that the PDMA proposal is not in total accord with this general proposed rule on electronic records and electronic signatures. As discussed in the preamble to the PDMA proposed rule (59 FR 11860),

FDA will consider the comments concerning electronic signatures and other signature substitutes received in response to both proposed rules before final rules are published.

4. Good Laboratory Practices

One comment suggested that a uniform definition of electronic identification would facilitate application of computer based automated systems in the area of GLP's.

One comment cited the language of 21 CFR 58.130(e) (of the GLP regulations) as calling for handwritten signatures of paper- based records, but allowing dated electronic identification for electronic systems.

FDA believes that, here again, broad acceptance regulations should resolve the issues related to GLP's.

VI. ACCEPTANCE REGULATIONS

Several comments asserted that a general rule with a broad preamble and specific targeted subsection changes would be the most efficient means of accepting electronic signatures throughout the applicable regulations. Other comments also supported new regulations that would accept electronic identification/signatures throughout existing FDA regulations. One comment suggested that FDA define the term electronic identification in the CFR in order to sanction use of those alternatives in place of handwritten signatures. Another comment said FDA's codified definition of signature should be clear yet general enough to allow industry the flexibility to use the most suitable technology. One comment said the agency should codify the terms signature, electronic signature, and electronic identification, provide examples of each term, and determine if there are substantive reasons for requiring handwritten signatures.

One comment suggested that to enhance the move from paper to electronic records, the agency should develop standards for the generation of portable electronic copies of records, copies that FDA may need in its enforcement activities. The comment also suggested that the agency require that systems be capable of generating such portable copies.

One comment suggested that regulations should consider an electronic record as "signed and final," once an operator endorses the record by entering a password.

One comment suggested that FDA's regulations would have to address both electronic integrity and administrative security. One comment urged that FDA's final publication resolve several specific issues regarding: (1) Elimination of paper documents when they are converted to electronic form, and distinguishing originals from copies; (2) establishing the "legal original" between secure electronic copies of conventionally signed paper documents; and (3) whether or not an operation can be based upon a combination of electronic and paper records.

One comment suggested that, until legal and security issues are resolved, the agency should accept electronic submissions, encourage development of electronic records systems, but require supplementary or accompanying handwritten, paper

based signatures. The comment added that such auxiliary endorsements would parallel the approach taken by the Internal Revenue Service regarding filing of electronic tax returns (based upon a conventionally signed paper form 8453) and would be relatively easy to implement. The same comment suggested that once electronic signatures are proven to be legally viable, FDA should not require them to be embodied in the electronic documents, but rather incorporated in supplementary documents so as to facilitate software modification. (As discussed in section VIII. of this document, one comment took the opposite view, stressing the importance of having the electronic signature securely bound to the signed document.)

One submission urged FDA to promulgate regulations regarding use of electronic signatures in the manufacture of blood components and subsequent testing and transfusion service laboratories. FDA agrees with the comments that called for broad regulations that would clearly define the terms handwritten signature and electronic signature (and do so in a manner that affords industry the greatest latitude in adopting appropriate technologies), and set conditions under which the agency would accept alternatives to handwritten signatures. The proposed regulations apply to all FDA program areas, including blood components, which are regulated as either drugs or medical devices.

The agency does not believe it necessary to define the term "electronic identification" because the general meaning of the term, as suggested by comments, would be contained in the proposed definition of electronic signature.

The agency agrees that it is vital for FDA to be able to obtain copies of electronic documents and that systems should have the capability of generating such copies--a provision that is in proposed § 11.10(b). However, the agency does not, at this time, agree that FDA needs to develop specific performance standards for the "portability" suggested. FDA may develop appropriate guidelines in the future to address portability attributes.

Regarding the suggestion that FDA require parallel paper records to bear mandated signatures pending resolution of legal issues, the agency believes that such a provision need not be codified because there are no indications that legal acceptance of electronic records/signatures (per se) remains an issue, where the trustworthiness/reliability of such records/signatures has been established. The proposed acceptance regulations address measures to establish such trustworthiness and reliability. However, until the regulations are in effect, firms must supplement electronic records with paper documents for purposes of having required signatures in conventional form.

The agency does not understand the basis for one comment's concern that electronic signatures not be required to be contained within the electronic records that are signed. The key factors in acceptability of electronic records/signatures have to do with establishing trustworthiness and reliability rather than facilitating software modification. Linking the electronic signature with the electronic document is an important attribute in establishing the authenticity of the endorsement, just as it is important to "affix" one's handwritten signature to a paper document. FDA believes

that electronic signatures which are separate from their associated writings are less reliable and trustworthy than electronic signatures which are incorporated in their respective documents, to the extent that authors can more easily repudiate the authenticity of the separated signature.

VII. ENFORCEMENT INTEGRITY

Most comments asserted that, based in part upon the provisions of Title 18 of the U.S. Code, use of signature alternatives should not adversely affect the agency's enforcement integrity. Comments asserted that laws against falsification of paper records apply equally to falsification of electronic records, and that FDA should have no difficulty in affixing individual responsibility when working with electronic records. Comments also maintained that electronic record systems must, and can under current technology, be designed for reliable storage and retrieval, thus meeting industry and FDA audit needs. Comments added that electronic record systems can be validated and are at least as reliable, and more efficient than, paper- based records.

One comment asserted that copies of electronic records containing signature alternatives will be admissible evidence, in regulatory actions, to demonstrate individual responsibility when FDA informs the industry that signature alternatives are as binding as conventional signatures.

One comment asserted that within the context of the PDMA, electronic signatures would be admissible in court when combined with other system controls, such as phoned requests.

The agency recognizes that the ability to collect electronic records that are admissible as evidence, depends in large measure on whether or not the systems used to generate those records have been designed for reliable storage and retrieval. Accordingly, the proposed regulations, at proposed § 11.10(c), require that systems that generate and maintain electronic records be designed so that the records can be reliably stored and retrieved. The storage/retrieval requirement should be coupled with the requirement that such systems be capable of generating accurate electronic copies that can readily be converted to human readable form. (See remarks on records "portability" in section VII.)

VII. SECURITY

Many comments contended that handwritten signatures are not intrinsically secure forms of identification because falsification can easily be executed unilaterally. Comments emphasized furthermore that properly validated and administered identification/password systems, which lack biometric links to individuals being identified, are more secure than handwritten signatures to the extent that falsification generally necessitates a bilateral action (i.e., two individuals must purposefully accomplish falsification). Comments asserted that security is fundamentally derived, not from the form of the identification, per se, but rather from the attendant system

controls.

One comment argued against placing too high an emphasis on security and control measures for signature alternatives, noting that FDA has not instituted corresponding controls for conventional handwritten signatures on paper records. The comment elaborated that isolated forgeries are more apt to go unnoticed than repetitive forgeries of a manual signature, and that security of habitual signing derives more from the meaning attached to the signing process than the technical strength of the process itself. The comment concluded that the effectiveness of electronic signature alternatives should also derive less from technical security and more from the meaning attached to the signing process.

The agency finds merit in the comments' premise that the integrity of an electronic signature is derived more from the systems controls used to generate it than from the technology used to apply it. The emphasis on systems controls is justified and reflected in the provisions of the proposed regulations. However, FDA recognizes that electronic signatures based upon biometric/behavioral links can be more secure than others to the extent they are more difficult to falsify. Whereas the agency agrees that the meaning attached to the signing process is important, (e.g., in establishing individual responsibility for an endorsed act such as approving a master production record), FDA does not agree that the meaning determines the security of the signing.

Regarding the comment that FDA has not instituted controls for the generation of handwritten signatures, the agency notes that specific FDA guidance on the matter has not been needed because conventional paper controls are well established in our culture and because falsification of paper documents can be readily investigated and documented by a long-standing body of forensic evidence (e.g., handwriting analysis, ink composition and dating, imprints on stacks of paper, erasure marks, etc.). On the other hand, a comparable body of evidence has yet to be established to pursue falsification of electronic documents and signatures.

The agency finds convincing the argument that electronic signatures based on user identification codes combined with passwords can be adequately secured in that the signature consists of multiple parts which require the collaborative efforts of two individuals to execute a falsification. FDA wishes to clarify, however, that contemporaneous use of both electronic signature elements must be executed for each signing. For example, if a person, having logged onto a system by entering both a password and a scanned employee badge containing an identification code, need only scan the badge to execute subsequent electronic signatures, then the safeguard of having multiple parts to the signature would be lost for those endorsements to the extent that another person could, unbeknownst to the badge owner, scan the badge and falsify the electronic signature. Should the owner carelessly leave the badge unattended, the required collaboration would be absent. On the other hand, if an "impersonator" needs to know the badge owner's secret password in addition to physically possessing the badge in order to execute a signing, then collaborative efforts would be necessary to falsify the electronic signature; the badge owner would have to reveal the password to the would-be-imposter, as well as make the badge

available. Accordingly, proposed § 11.200(a)(1) requires electronic signatures that are not based on biometric/behavioral links to employ at least two distinct parts, all of which are contemporaneously executed at each signing. In addition, proposed § 11.200(a)(3) requires that attempts at signature falsifications necessitate collaboration of at least two people.

The agency believes that the acceptance regulations need not require at least two distinct elements where the electronic signature employs a biometric/behavioral link (e.g., retinal scan, voiceprint) to the signer. The bilateral security measure would not be necessary in such systems because only the genuine owner of the electronic signature would be capable of using it. The owner could not lose, lend, give away or otherwise transfer the signature in the first place.

One comment expressed the hope that security for alternatives to handwritten signatures will not result in lesser confidentiality.

FDA agrees that confidentiality of data in electronic records is as important as it is in paper records. Systems controls, for both paper and electronic documents, will determine the level of confidentiality.

One comment stated that signatures recorded electronically, if not somehow inalterably bound to the electronic document, are insecure to the extent the digitally recorded signature could be excised and superimposed upon other documents to falsify an endorsement. Another comment supported signatures recorded electronically when they are captured to inalterable media, such as optical disks, provided further, that access to such media is limited, thus reducing chances of alteration.

The agency agrees that binding an electronic signature to the signed electronic document is a vital systems control that helps to establish the authenticity of an electronically signed document. Accordingly, proposed § 11.70 includes a "signature to document" binding provision. FDA notes that such a binding is usually inherent for handwritten signatures that are applied to paper documents.

As noted above regarding stratification, many comments made a distinction between the security needed for signature alternatives affixed to electronic documents contained within the administrative control of a given firm (closed system) and signature alternatives affixed to records (such as e-mail and submissions to FDA) that are transmitted from one establishment to another (open systems). Comments suggested that open systems require a higher level of security than closed systems, and that a combination of user identification codes and passwords, under suitable administrative controls, is sufficient for closed systems.

The agency agrees that because open systems are inherently more vulnerable to message compromise, additional security measures may be necessary to ensure electronic document integrity and authenticity. Such measures may include electronic document encryption and use of digital signatures. However, FDA believes that because such measures are still evolving, it would be premature to specifically require their use in documents submitted electronically to the agency. Instead, the proposed rule requires additional security measures, stated in general terms, that are designed

to ensure document integrity, confidentiality, and authentication from point of creation to point of receipt.

One comment suggested that computer systems used within the CGMP and GLP regulations attain the security level of C2 within the Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28--STD), also known as the "Orange Book." One comment concluded that, per the ANPRM working definitions, signatures recorded electronically (scripted signatures applied to devices other than paper) and conventional signatures applied to paper offer the greatest security.

FDA does not believe it necessary at this time to codify adherence to a specific security level that is stated in a standard. The agency believes that records under CGMP's and GLP's will have sufficient security when the provisions of the proposed rule are followed. However, should additional specific criteria be necessary to attain adequate levels of security, the agency may consider incorporating specific security standards such as the one suggested.

Many comments identified various administrative security controls attendant to the use of (what the ANPRM called) electronic identification (identification codes (ID)/passwords), and argued that appropriate use of such controls should make ID/password systems acceptable to FDA for use in closed systems. Comments generally emphasized the need to utilize such controls and not rely upon a single form of signature alternative in isolation. Suggested controls included the following:

1. Establish and follow employee policies which hold people accountable and liable for actions initiated under their (computer ID) accounts to deter forgery of electronic signatures. Comments suggested that employees who violate such policies would be subject to disciplinary action including termination.
2. Limit computer access to authorized individuals.
3. Execute carefully written and controlled operational procedures.
4. Train employees in the use of operational procedures.
5. Use fully documented production and control procedures.
6. Validate systems.
7. Use identity checks; cross-checking to establish that machine readable codes on tokens and a personal identification number (PIN) are assigned to the same individual.
8. Use password checks; checking an independently entered password.
9. Change passwords periodically.
10. Use authority checks to determine if the identified individual has been authorized (or trained) to use the system, access, or operational device, or perform the operation at hand.
11. Use time stamped audit trails to document changes, record all write-to-file operations, and independently record the date and time of the operator's action or entry. Concerning audit trail integrity, comments emphasized the importance of creating back up files to re-create documentation and deter inappropriate records alterations.
12. Use operational checks to enforce permitted operational parameters such as

functional sequencing or time.

13. Use records revision and change control procedures to maintain an electronic audit trail that documents time-sequenced development and modification of records.

14. Maintain control over the distribution, access, and usage of documentation required for various operations.

15. Encrypt records to provide secure, nonchangeable versions.

16. Use location (terminal) checks to determine that the physical source of the endorsement is valid.

17. Use intentions checks by providing confirming dialog that the signer understands precisely the intentions of a signature.

18. Use "time-outs" of under-utilized terminals to prevent their unauthorized use while unattended.

19. Use security against natural system failures.

20. Print the individual's name, along with time of "signing," on the electronic record to help reenforce the psychological link between the author and the endorsement.

The agency considers that most of the above systems controls have merit and they have been incorporated in the proposed regulations.

One comment identified the following steps to regulate and control the issuance of tokens, cards, PIN's, and other machine readable indicia of identity:

1. Chronological logging of each issuance;
2. Certifying the identity of each individual;
3. Noting and controlling the empowerment or authority of issuance;
4. Testing each token, card, or other indicia to make sure it works;
5. Keeping each issuance unique;
6. Assuring that issuances are periodically checked, recalled, or reissued;
7. Following loss management procedures to electronically de-authorize lost tokens, cards, etc, and to issue temporary or permanent replacements using suitable, rigorous controls for substitutes; and,
8. Using reasonable transactional safeguards to prevent unauthorized use and detect and emergently report (with unmistakable notoriety) any unauthorized attempts.

The agency agrees that all of the above controls are reasonable and necessary measures to maintain password integrity. However, some of these controls may be more amenable to incorporation in guidelines rather than regulations, and therefore do not appear in the proposed rule.

In response to the ANPRM's request that comments identify any types of signature alternatives that would be too insecure to be acceptable, comments cited the use of unilateral methods, such as a user identification that is readily determined from a publication, or alternatives used in environments in which employees are motivated to falsify identifications. One comment stressed the importance of using bilateral systems, but urged the agency to permit industry to choose the exact methods (such as use of identification codes combined with passwords or tokens). As explained above, the agency agrees that single entity signature alternatives that may be compromised are not acceptable. Where bilateral signatures are used, both portions of

the signature should be recorded contemporaneously with each "signing." Absent that duality, FDA would consider the signature to be unilateral and therefore, if capable of being compromised, unacceptable. The agency wishes to clarify, however, that single entity signatures based on biometric/behavioral links that cannot be implemented by people other than their genuine owners would be acceptable.

VIII. VALIDATION

Comments generally acknowledged the importance of validating signature alternative systems and said that there should be no difference between validation of signature alternatives and validation of other processes or systems. Most comments claimed that there already exists sufficient guidance, published by FDA and the industry, thus making it unnecessary for FDA to publish additional guidance on validation of signature alternatives. Several comments acknowledged FDA's concerns about the adequacy of computer systems validation, but indicated that the primary issue concerns what constitutes adequate systems specifications, a matter comments claimed is still developing. Comments identified the following elements of signature alternative validation:

1. Correct specification;
2. Correct engineering;
3. Correct testing;
4. Correct operation;
5. System definition: functional requirements, software requirements, the physical system and its operating environment;
6. Assurance of software quality: structural and functional;
7. System documentation that is well organized and that includes policies, procedures and master plans defining the philosophy and approach to system validation, and defined meanings for approval signatures;
8. Security;
9. Verification of critical data entries;
10. Installation, operational, and performance qualification;
11. Change control and system maintenance;
12. Employee training;
13. A records retrieval system that protects records and enables their accurate and efficient retrieval throughout their retention period; and
14. Periodic system review and revalidation.

The agency is persuaded by the comments that although validation of electronic signature systems is important enough to be codified as a general requirement, publication of specifics as to what constitutes acceptable validation of such systems should be deferred at this time. Specific information on electronic signature validation may need to be provided in either future regulations and/or guidelines.

IX. STANDARDS

A. Standards in General

Several comments acknowledged the general utility of standards (e.g., for electronic signatures which use biometric/behavioral links), but suggested that the issue should be addressed separately on the basis that standards are not relevant to the forms of electronic identification anticipated for use in the pharmaceutical industry, and because they are seldom used in FDA-regulated industries generally.

Several comments said FDA should assess existing standards and provide input into development of new standards, but should not seek a lead role in their development. One comment suggested that FDA collaborate with industry in developing standards should they be warranted in the future.

Two comments argued that the absence of standards should not inhibit the agency from accepting electronic identification and that standards would not be necessary where there is an emphasis on validation, security, and well designed and enforced procedures.

One comment urged the agency to avoid adopting any single standard or technology for electronic signatures.

FDA recognizes the benefits of standards and their relevancy to legal and regulatory acceptance of electronic signatures. FDA regulations could be simplified by predicating acceptance of an electronic signature on adherence to one or more appropriate standards that have been derived from fair evaluation of public comments. Although industries regulated by FDA may not have participated in the development of the two emerging primary digital signature standards, i.e., the National Institute of Standards and Technology Digital Signature Standard (NIST DSS) or the RSA, either because (in the case of the RSA) the standard is proprietary, or because the industry did not anticipate their relevancy, the standards may nonetheless be valuable tools to ensure the authenticity and integrity of electronic records. In general, the agency agrees with the premise that adherence to specific standards need not be codified at this time because adequate levels of security may be achieved by adherence to the controls contained in the proposed rule. However, the agency may need to address or adopt such standards in the future, as the industries become more familiar with them and their practical applications. The agency anticipates that its role will be that of a proactive participant in standards development. Absent the immediate application of such standards, the proposed rule emphasizes, as comments suggest, system security/integrity controls, and validation.

B. National Institute of Standards and Technology Digital Signature Standard

One comment suggested, without elaboration, that FDA obtain and consider three cited articles on digital signature standards. Many comments cited the controversial nature, per published articles, of the NIST DSS and suggested that FDA not adopt the

standard. Several comments inferred that FDA should favor the RSA over the NIST DSS on the basis that RSA is currently the de facto standard for commercial and some military applications. One comment urged the agency to adopt a public, rather than proprietary standard, but noted the difficulty of modifying systems that are essentially completely developed to incorporate the NIST standard.

One comment encouraged FDA to adopt the NIST draft digital signature standard, on the grounds that the NIST DSS is a highly secure method of identification that will become mandatory for Federal agencies where a public-key based digital signature technique is needed and is to be the single standard for Government communication with the private sector. The comment further supported the standard by noting its acceptance by the General Accounting Office as legal endorsement for Federal obligations. In addition, the comment asserted the nonrepudiation property of the NIST DSS. One comment acknowledged that the NIST standard offers the benefit, over handwritten signatures, of assuring that the document was not altered after being signed by the author.

The agency notes that subsequent to the working group's February 1992 progress report, several criticisms of the NIST DSS, specifically the absence of a "hash algorithm" and limited size of "keys," have been addressed. FDA has also become aware of several commercial products available to implement the standard, and the agency acknowledges that it may have direct applicability to FDA electronic communication with the agency's regulated industries. However, the standard is not yet finalized, and it has not yet achieved sufficiently wide utilization, in the agency's opinion, to merit mandatory use, at least in closed systems. The standard may have future applicability, though, in open systems, where documents are submitted to FDA via public electronic carriers, in which case adherence to a limited number of standards would be desirable to maintain practical communications. Accordingly, the agency is deferring a codified reference to the NIST DSS in particular. However, the agency is proposing in § 11.30 to use established digital signature standards that are acceptable to FDA, as a system control that may be warranted to maintain record authenticity, integrity, and confidentiality in open systems.

X. FREEDOM OF INFORMATION

Several comments asserted that because matters relating to FOI are not relevant to the fundamental issues of electronic identification, such issues should be handled separately. However, comments expressed concern about the reliability of computer methods FDA might use to delete proprietary information from electronic records released under the FOI Act.

Two comments said that FDA should realize FOI processing cost savings when records are submitted electronically if the agency sets guidelines on such submissions.

Comments held diverse opinions about what form (electronic or otherwise) documents released under FOI should take. Several comments said FDA should establish standards to avoid having to copy and purge original records that exist in

many different formats. Some comments said they would likely provide paper printouts of electronic records requested by FDA field investigators, and by so doing, the agency would not need to acquire specific software and hardware to handle proprietary formats. Likewise, two comments recommended that FDA respond to FOI requests by providing only paper copies of documents, regardless of the format requested. On the other hand, two comments encouraged the agency to develop systems whereby requesters could submit FOI requests by e-mail, or directly access an FDA data base to conduct on-line text searches. One of the comments suggested that resulting documents from such searches be mailed to requesters in a manner similar to the procedure used by the National Library of Medicine's Medline. The respondent suggested that modest connect time fees would be appropriate to such systems.

The agency disagrees with the assertion that FOI matters are irrelevant to electronic signature issues. When FOI requests are received electronically the agency must ensure that the requests are authoritative and genuine such that they may be processed and appropriate fees collected. In addition, as more firms implement electronic records, the agency will likely collect and store them electronically in the regular course of its investigational and inspectional activities. The consequent move from paper to electronic documents will necessitate use of appropriate purging technologies, as many of the comments have noted.

FDA finds the comment's suggestions that FOI records be handled strictly as paper documents inconsistent with the implementation of electronic records systems. The agency believes the suggestion that FDA accept FOI requests by e-mail has merit, and it is exploring ways of implementing the suggestion within the context of electronic submissions in general. A data base of all available documents may not be practical at this time considering the scope of potential documents that may be in the data base. However, a publicly accessible on-line electronic data base of FOI-released documents may be in the public interest, and this suggestion may also be explored. The agency agrees that it should set technical standards for submission of electronic documents so as to allow the electronic handling of relevant FOI requests; this suggestion is also being explored within the context of electronic submissions in general.

XI. THE PROPOSED REGULATION FOR ELECTRONIC SIGNATURES AND RECORDS

Proposed part 11 is made up of the following subparts: subpart A--General provisions; subpart B--Electronic records; and subpart C--Electronic signatures:

A. General Provisions (Subpart A)

1. Scope (§ 11.1)

Although most of the comments to the ANPRM represented the pharmaceutical

industry, the agency wishes to emphasize that the proposed rule applies to use of electronic records and signatures in the context of all FDA program areas and all industries regulated by FDA. Accordingly, proposed § 11.1 states the extent of the regulation's scope to all parts of 21 CFR chapter I. The agency recognizes, however, that in some instances records required by selected sections of chapter I may need to be retained in paper form and their associated conventional methods of signing may need to be preserved. In such instances, the agency would, by regulation, specify that electronic versions of those records would not be permitted. FDA does not anticipate many such situations, but is providing for them in proposed § 11.1. The agency welcomes comments on any existing FDA regulations that address records where electronic versions of those records should not be permitted.

Under proposed § 11.1, absent specific exemption by regulation, records required throughout chapter I could be created, modified, maintained, or transmitted in electronic form provided they meet the requirements of proposed part 11. Likewise, electronic signatures would be considered to be equivalent to full handwritten signatures, initials, and other general signings required throughout chapter I provided the electronic signatures and associated electronic records meet the requirements of the proposed part 11.

2. Implementation (§ 11.2)

The agency recognizes that the pace and extent of converting from paper to electronic records will vary significantly in industry and, in fact, within FDA itself. Adoption of electronic records technologies generally depends upon a number of factors, including systems availability, costs, integration into existing paper based records systems, and the need to train employees in developing and maintaining electronic systems. In order to implement the new rule in a fair and practical manner, the agency is dividing the types of records to be covered into two broad categories, namely records required by regulation to be maintained but not submitted to FDA (such as batch production records), and records submitted to FDA (such as food additive petitions and comments to proposed rules).

This approach is being taken for two reasons. First, the agency believes it is important to enable regulated industries to implement electronic records/signatures for records that are required by regulation to be maintained, but not submitted to the agency, as rapidly as possible. Some firms have already taken major steps toward implementing electronic production records and the agency does not wish to delay the appropriate adoption of new technologies.

Second, FDA is not yet prepared to accept and manage all submissions in electronic form. However, FDA believes it vital to enable those agency units that are prepared to receive and manage submissions in electronic form to do so as rapidly as practical. There are many different types of submissions to the agency. (A July 1991 FDA report entitled, "Basic Inventory of Submissions to the FDA," (Office of Planning and Evaluation) identified 87 different types of submissions (Ref. 4)). The agency is

reviewing all of the various submissions to identify which documents it can accept and manage in electronic form (in whole or in part), and the corresponding capabilities of the receiving agency units. The agency is committed to accepting as many submissions in electronic form as possible, consistent with available resources, but realizes that the goal of accepting all submissions in electronic form will be achieved in phases over a period of time.

The agency intends to publish a public docket on electronic submissions (docket number to be announced). The docket would identify those submissions that may be made (in whole or in part) in electronic form, and the corresponding agency receiving units. Receiving units may also publish appropriate technical guidance documents on how submissions are to be made relative to the units' capabilities. In addition, FDA encourages submitters to work with the agency to develop appropriate pilot programs to implement electronic submissions that may be more complex in nature. The agency is committed to the goal of eventually accepting most submissions in electronic form because it recognizes the attendant benefits of using electronic records, benefits such as speedier document review times, cost savings in not having to store and manage paper, and the improved responsiveness to the general public and regulated industries that generally derives from electronic systems.

Therefore, proposed § 11.2(a) enables persons to use electronic records/signatures in lieu of paper records/conventional signatures, in whole or in part, for records which are required by FDA regulation to be maintained, but not submitted to FDA. Proposed § 11.2(b) enables persons to use electronic records/signatures in lieu of paper records/conventional signatures, in whole or in part, for records that are submitted to FDA, provided the type of submission has been identified in public docket (docket number to be announced) as one which FDA accepts in electronic form. The agency intends to announce changes to the public docket, on a periodic basis, by a variety of means. For example, a notice announcing changes may be published in the FEDERAL REGISTER.

FDA wishes to clarify that the requirements in proposed part 11 would apply to both types of electronic records (submissions FDA accepts in electronic form and records required by regulation to be maintained) unless, as stated above, a regulation specifically prohibits the record from being in electronic form.

3. Definitions (§ 11.3)

Proposed § 11.3 sets forth definitions of key terms, including "biometric/behavioral links," "closed system," "open system," "electronic record," "electronic signature," and "handwritten signature."

A "biometric/behavioral link" (proposed § 11.3(b)(3)) is a method of verifying a person's identity based on measurement of the person's physical feature(s) or repeatable action. The agency believes that biometric/behavioral links would be utilized in technologies that use, for example, voiceprints, handprints, and retinal scans to identify individuals. A system that characterizes the act of signing one's name, as a

function of unique behavior (parameters of physical signing such as speed of stylus movement, pressure, pauses, etc.) is another example. A fundamental premise of biometric/behavioral link technologies is that the resulting electronic signatures are inherently unique to an individual and cannot, by ordinary means, be falsified. A "closed system" (proposed § 11.3(b)(4)) is an environment in which there is communication among multiple persons, where 71 system access is restricted to people who are part of the organization that operates the system. FDA believes that electronic documents within a closed system are less likely to be compromised than those in an "open system" because they are not as vulnerable to disclosure to, and corruption by, unintended outsiders to the organization. Where a firm hand delivers to FDA a magnetic disk containing an electronic document, the agency would consider such communication to have been made in a closed system.

An "open system" (proposed § 11.3(b)(8)) is an environment in which there is communication among multiple persons, where system access extends to people who are not part of the organization that operates the system. FDA believes electronic documents in open systems merit additional protection from unauthorized disclosure and corruption. Where a firm sends FDA an electronic document by electronic mail, the agency would consider such submission to have been made in an open system. An "electronic record" (proposed § 11.3(b)(5)) is 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. The agency is proposing a broadly based definition of this term in order to accommodate digital technologies that may incorporate pictures and sound, in addition to text and data.

Although, as discussed above, the ANPRM discussed four possible terms relating to different kinds of signatures, FDA is proposing two definitions based broadly on whether or not the "signature" is handwritten. Two definitions are proposed, one for "electronic signature" (§ 11.3(b)(6)) and one for "handwritten signature" (§ 11.3(b)(7)). The term electronic signature would include the meaning comments ascribed to electronic identification. Handwritten signatures would include signatures recorded electronically.

Proposed § 11.3(b)(6) defines the term "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. The fundamental premise is that an electronic signature is some combination of what a person possesses (such as an identification card), knows (such as a secret password), or is (the unique characteristic embodied in a biometric/behavioral link such as a voiceprint).

Proposed § 11.3(b)(7) defines the term "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. An important aspect of a handwritten signature is that the act of signing with a writing or marking instrument such as a pen, or stylus is preserved. The agency is aware of electronic records

systems which capture the image of a signature as a person applies a handwritten signature to a "screen" or sensing device. Because the traditional action of signing is preserved, the agency regards such a signature to be a handwritten signature even though it is written to an electronic document. The proposed definition includes wording to clarify this intent.

B. Electronic Records (Subpart B)

As discussed above, the agency has accepted the comments on the ANPRM that suggested that adequate system controls should be the basis for establishing the regulatory and legal acceptance of electronic records. The agency appreciates the extent of the suggested controls which are intended to ensure the authenticity, integrity, and confidentiality of electronic records and to ensure that signers cannot readily repudiate the electronic records as not genuine. FDA has incorporated most of the controls in the proposed regulations. Controls not adopted at this time may be incorporated in subsequent revisions to these regulations, or addressed in agency guidelines. In addition, FDA accepts the premise that some stratification of those controls should be codified based upon whether the electronic records are within closed or open systems. Therefore, this subpart includes separate controls for records in closed and open systems.

1. Controls for Closed Systems (§ 11.10)

Proposed § 11.10 includes a general requirement that there be 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. In addition, the agency is proposing 11 specific controls.

FDA wishes to emphasize that the proposed list of system controls is not intended to be all inclusive of what may be needed for a given electronic records system, and that some controls may not be necessary in all types of systems. The wording of the proposal is intended to clarify which controls are generally applicable and which are germane to certain types of systems depending upon their intended use. For example, operational checks to enforce permitted sequencing of events would not be appropriate to systems in which proper sequencing was not relevant to the events being recorded. Examples of system controls that would be applicable in all cases include validation and protection of records to ensure that records remain accurate and retrievable throughout their retention period.

Some of the proposed system controls (e.g., inspection and copying of records) are necessary to ensure that the agency can fulfill its enforcement responsibilities. The subject of enforcement integrity was extensively addressed in the ANPRM and by comments, most of whom asserted that properly validated and secured systems should not hamper the agency's enforcement activities.

As discussed above, many ANPRM comments asserted that enforcement integrity would not be hampered because, under Title 18 of the U.S. Code, falsification of electronic records would be equivalent to falsification of paper records.

The agency agrees that certain controls, such as system validation, are necessary to maintain the integrity of electronic documents it reviews and collects as part of its enforcement activities. It is also necessary for FDA to be able to review and copy electronic records in the same manner as paper records. Accordingly, the proposed rule contains several provisions designed to ensure that the agency's enforcement responsibilities are not impeded. For example, proposed § 11.10(b), regarding the ability to generate true copies of electronic records that FDA can inspect, review, and copy, is intended to ensure that the agency will retain the ability to review electronic records on site and review copies of such records off site, in the same manner as is currently the case for paper records. Likewise, proposed § 11.10(e), regarding time stamped audit trails to document record changes, is intended to ensure that changes to electronic records are evident and reviewable by the agency, to the same extent as paper records.

The agency encourages persons to consult with FDA prior to implementing electronic records systems if there are any questions regarding the ability of the agency to review and copy the electronic records. The proposed rule includes wording to that effect.

2. Controls for Open Systems (§ 11.30)

As discussed above, many comments to the ANPRM acknowledged that additional security measures, above and beyond those used for closed systems, may be needed to ensure the integrity, authenticity, and confidentiality of electronic records within open systems.

The agency agrees. FDA is aware that two kinds of additional systems controls can be effective in this regard--use of document encryption, and use of digital signature standards. Digital signature standards use established mathematical algorithms and public and private signer numerical codes (called keys) to both authenticate an electronic record and establish its integrity. Several comments addressed these additional measures. Accordingly, proposed § 11.30 requires use of those controls identified in proposed § 11.10 for closed systems (as appropriate to the nature of the records at issue) plus such additional measures as document encryption and use of digital signature standards acceptable to FDA, as necessary to maintain record confidentiality and integrity under the circumstances. The agency intends to publish future guidance documents which identify acceptable digital signature standards.

3. Signature Manifestations (§ 11.50)

Proposed § 11.50 requires several of the system controls suggested by comments to the ANPRM. This section requires electronically signed records to display the

printed name of the signer and the date and time when the document was signed. The presence of the printed name, date, and time will assist the agency by clearly identifying the signing individual. In addition, the printed information will help firms to maintain an unambiguous method of readily and directly documenting the signer's identity and date of signing for as long as the electronic record is retained. Another benefit to having the name of the signer appear on the electronic document is to reinforce the solemnity and personal commitment associated with the act of signing.

Proposed § 11.50 also requires that the meaning associated with the act of signing the electronic document be clearly indicated. As discussed in the ANPRM, the purpose of a signature can be varied (e.g., to affirm, review, approve, or indicate a person's presence or action). Many traditional paper records already contain statements that indicate the purpose of a signature, such as "material added by * * *," "in witness thereof," and "approved by * * *." The agency believes it is vital, for purposes of accurate documentation and establishment of individual responsibility, to include such statements in electronic records as well.

4. Signature/Record Binding (§ 11.70)

Signatures appearing on conventional paper documents cannot be readily excised, copied, or transferred to other documents so as to falsify another document. Attempts at such misdeeds can generally be revealed by available forensic methods. Such is not typically the case, however, with electronic signatures and handwritten signatures executed to electronic records (the image of the signature may be electronically "copied" from one location and "pasted" to another without evidence of the action.) In such cases, falsification of electronic documents would be relatively easy to achieve, yet difficult to detect. This problem could be solved by using available technologies to bind the signature to the electronic document in a secure manner analogous to the way conventional signatures are affixed to paper records.

As discussed above, two ANPRM comments specifically addressed signature to record binding. One comment stated that signatures recorded electronically, if not somehow inalterably bound to the electronic document, are insecure to the extent the digitally recorded signature could be excised and superimposed upon other documents to falsify an endorsement. Another comment supported signatures recorded electronically when they are captured to inalterable media, such as optical disks, provided, further, that access to such media is limited, thus reducing chances of alteration.

The agency agrees with the ANPRM comments and believes it is vital to verifiably bind a signed electronic record to its electronic or handwritten signature. Accordingly, proposed § 11.70 includes a "signature to document" binding requirement to ensure that the signatures cannot be excised, copied or otherwise transferred so as to falsify another record. The agency believes that such binding is readily achievable under current technology. For example, the concept of such binding is part of digital signature standards to the extent that a message authentication operation will fail for a

falsified document if the document's digital signature had been copied from a different document.

C. Electronic Signatures (Subpart C)

Proposed subpart C includes requirements for system controls that are relevant to electronic signatures. Here, as elsewhere throughout the proposed rule, the controls reflect suggestions made by the ANPRM comments. In addition, the agency is including a requirement for providing certification to the agency that the electronic signature systems and, if necessary, specific electronic signatures are authentic, valid, and binding.

1. General Requirements (§ 11.100)

Proposed § 11.100 requires each electronic signature to be unique to one individual and requires the issuing authority (for example, a systems security unit within a firm) to verify a person's identity before issuing an electronic signature. FDA considers these controls to be fundamental to the basic integrity of an electronic signature. Uniqueness is important because, if two or more people are assigned the same electronic signature (such as a combination of identification code and password) then the true identity of the signer could be in doubt and either of the two individuals could conceivably readily repudiate the recorded signature as not being his/her own. It is important for the assigning authority to verify a person's identity before issuing an electronic signature to prevent that person from wrongfully assuming someone else's identity and the privileges/authorizations that may be associated with that identity.

The agency is including a proposed requirement for providing certification to the agency that the electronic signature system guarantees the authenticity, validity, and binding of any electronic signature. Furthermore, upon agency request, additional certification or testimony that a specific electronic signature is authentic, valid, and binding shall be provided. The certification should be submitted to the agency district office in which territory the electronic signature system is in use.

2. Identification Mechanisms and Controls (§ 11.200)

As noted above, electronic signatures are broadly based upon various combinations of what a person knows (such as a secret password), what a person possesses (such as an employee badge), and what a person is. The third element, what a person is, relates to what the agency is defining as a "biometric/behavioral link" to an individual--a method of verifying a person's identity based on measurement of the person's physical feature(s) or repeatable actions. Examples of such features or actions include voiceprints, handprints, retinal scans, and the act of signing one's name in script. The most important attribute of an electronic signature that incorporates a biometric/behavioral link is that the measured feature or action is inherently unique to,

and remains with, that individual. Unlike what a person knows or possesses, what a person "is" cannot be compromised by being lost, stolen, forgotten, loaned, re-assigned, or otherwise compromised by ordinary means.

Accordingly the agency is establishing two broad categories of electronic signatures, those based on biometric/behavioral links to individuals, and those that lack such links, as reflected in proposed § 11.200.

Many of the ANPRM comments argued persuasively that FDA should not require biometric/behavioral links, but should accept electronic signatures that lack such links provided the electronic signatures are validated, secure, and administered under adequate system controls. Among those controls, comments emphasized the importance of maintaining electronic signatures that are made of multiple identification mechanisms (such as a combined identification code and password) and administrative measures to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. Such collaboration would prevent signature falsification by casual mishap--a falsification that might result, for example, if someone acquired another person's unattended identification card or token. The provision would also help to impress people with the significance and solemnity of the electronic signature. The agency agrees that biometric/behavioral links should not be a required feature of electronic signatures, at this time. The agency also agrees that electronic signatures that lack biometric/behavioral links should be acceptable when certain system controls are used. Accordingly, the agency has incorporated system controls for electronic signatures that lack such links, including multiple identification mechanisms and multiple party collaboration in proposed § 11.200(a).

Although FDA is not, at this time, mandating use of biometric/behavioral links in electronic signatures, it is allowing for them and encourages their development and use. The premise behind the technology for electronic signatures based upon biometric/behavioral links is that the links are inherently secure such that a person's electronic signature could not be lost, stolen, loaned, or otherwise used by anyone other than the rightful owner. The agency is proposing to codify that premise at § 11.200(b), to ensure that electronic signatures based on such links are designed so that they cannot be used by anyone other than their genuine owners.

3. Controls for Identification Codes/Passwords (§ 11.300)

The agency is aware that many electronic signatures are based upon combined identification codes and passwords. FDA believes that because of the relative ease with which such electronic signatures may be compromised, and because of their wide adoption, system controls to ensure their security and integrity merit specific coverage in these regulations.

Many of the ANPRM comments addressed specific administrative controls to ensure the security and integrity of electronic signatures that are based upon a combined identification code and password. One comment suggested eight controls

specific to identification codes. The agency appreciates the various suggestions and agrees that five of them merit codification at this time. Proposed § 11.300 includes those controls. Suggested controls that were not included in the proposed rule may be added in the future or addressed in future agency guidelines.

The agency wishes to emphasize that the controls listed in proposed § 11.300 are not intended to be all inclusive of what may be needed to ensure the security and integrity of electronic signatures based on identification codes/passwords.

XII. ANALYSIS OF IMPACTS

FDA has examined the impacts of the proposed rule under Executive Order 12866 and the Regulatory Flexibility Act (Pub. L. 96-354). Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distribute impacts; and equity). The agency believes that this proposed rule is consistent with the regulatory philosophy and principles identified in the Executive Order. In addition, the proposed rule is not a significant regulatory action as defined by the Executive Order and so is not subject to review under the Executive Order.

The Regulatory Flexibility Act requires agencies to analyze regulatory options that would minimize any significant impact of a rule on small entities. Because this action will permit industry to maintain records in electronic form, and thus reduce their paperwork costs, the agency certifies that the proposed rule will not have a significant economic impact on a substantial number of small entities. Therefore, under the Regulatory Flexibility Act, no further analysis is required.

XIII. PAPERWORK REDUCTION ACT OF 1980

This proposed rule contains information collections which are subject to review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1980. The title, description, and recordkeepers of the information collections are shown below with an estimate of the recordkeeping burden.

Title: Electronic Records; Electronic Signatures; Title 21 Code of Federal Regulations; Proposed Rule.

Description: The Food and Drug Administration (FDA) is proposing rules to provide criteria for acceptance of electronic records, electronic signatures, and handwritten signatures onto electronic records useable in place of paper records. Rules apply to any 21 CFR records retention requirement unless specifically exempt by future regulation. Records required to be submitted to FDA may be submitted electronically provided the agency has stated its ability to accept the records electronically in an agency established public docket.

Description of Recordkeepers: State or local governments, businesses and other

for-profit organizations, Federal agencies, and non-profit institutions.

Estimated Annual Burden for Recordkeeping

21 CFR Section	Number of recordkeepers	Hours per recordkeeper	Total Burden hours
11.10	50	40	2000
11.30	50	40	2000
11.50	50	40	2000
11.300	50	40	2000
Total annual burden hours			8,000

As required by section 3504(h) of the Paperwork Reduction Act, FDA is submitting to OMB a request that it approve these information collection requirements. Organizations or individuals desiring to submit comments for consideration by OMB on these information collection requirements should address them to FDA's Dockets Management Branch (address above) and to the Office of Information and Regulatory Affairs, OMB, rm. 3208, New Executive Office Building, Washington, DC 20503, Attn: Desk Officer for FDA.

XIV. ENVIRONMENTAL IMPACT

The agency has determined under 21 CFR 25.24(a)(8) that this action is of a type that does not individually or cumulatively have a significant effect on the human environment. Therefore, neither an environmental assessment nor an environmental impact statement is required.

XV. REFERENCES

The following references have been placed on display in the Dockets Management Branch (address above) and may be seen by interested persons between 9 a.m. and 4 p.m., Monday through Friday.

1. FDA, Task Force on Electronic Identification/Signatures, Electronic Identification/Signature Working Group Progress Report, February 24, 1992.

2. National Performance Review, Report of the Vice President pp. 113-117, September 7, 1993.

3. FDA, Letter to Pharmaceutical Manufactures Association, December 5, 1991.

4. FDA, Office of Planning and Evaluation, "Basic Inventory of Submissions to FDA," July 1991.

XVI. COMMENTS

Interested persons may, on or before November 29, 1994, submit to the Dockets Management Branch (address above) written comments regarding this proposal. Two copies of any comments are to be submitted, except that individuals may submit one copy. Comments are to be identified with the docket number found in brackets in the heading of this document. Received comments may be seen in the office above between 9 a.m. and 4 p.m., Monday through Friday. As an FDA experiment in accepting public comments by electronic mail (e-mail), interested persons may also submit comments via INTERNET (address above). Comments must be in ASCII format. Any exhibits or other attachments submitted must also be in ASCII format and must be part of the e-mail itself. The agency has limited experience with receiving e-mail via INTERNET, and is aware that it is possible for some messages not to arrive at their intended destinations, or to arrive with incomplete or otherwise inaccurate contents. FDA is concerned that all comments it receives on this proposal are intact, accurate and complete, as intended by respondents. Therefore, for this experiment, FDA encourages interested persons who elect to send their comments by e-mail to also send two paper copies of their comments to the Dockets Management Branch (address above).

List of Subjects in 21 CFR Part 11

Administrative practice and procedure, Electronic records, Electronic signatures, Reporting and recordkeeping requirements. Therefore under the Federal Food, Drug, and Cosmetic Act, and under authority delegated to the Commissioner of Food and Drugs, it is proposed that 21 CFR part 11 be added to read as follows:

Part 11--ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A--General Provisions

Sec.

Subpart B--Electronic Records

Subpart C--Electronic Signature

AUTHORITY: Secs. 201-902 of the Federal Food, Drug, and Cosmetic Act, 52 Stat. 1040 et seq., as amended (21 U.S.C. 301- 392).

Subpart A--General Provisions

§ 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the Food and Drug Administration considers electronic records, electronic signatures, and handwritten signatures executed to electronic records, to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) These regulations apply to records in electronic form that are created, modified, maintained, or transmitted, pursuant to any records requirements set forth in chapter I of this title.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required throughout this chapter, unless specifically exempted by regulation that is effective on or after the effective date of this part.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper based records, in accordance with § 11.2, unless paper based records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained pursuant to this part shall be readily available for, and subject to, FDA inspection.

§ 11.2 Implementation.

(a) 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, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic

records/signatures in lieu of paper records/conventional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts(s) of a document to be submitted has/have been identified in public docket (docket number to be determined) as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic format without paper records and to which specific receiving unit(s) of the agency (e.g., specific center, office, division, branch) such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons should consult with the intended agency receiving unit for details on how and if to proceed with the electronic submission.

§ 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-902, 52 Stat. 1040 et seq., as amended (21 U.S.C. 301- 392).

(2) Agency means the Food and Drug Administration.

(3) Biometric/behavioral links means a method of verifying a person's identity based on measurement of the person's physical feature(s) or repeatable action(s).

(4) Closed system means an environment in which there is communication among multiple persons, where system access is restricted to people who are part of the organization that operates the system.

(5) Electronic record means 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.

(6) Electronic signature means 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.

(7) Handwritten signature means 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. However, the scripted name, while conventionally applied to paper, may also be applied to other devices which capture the written name.

(8) Open system means 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.

Subpart B--Electronic Records

§ 11.10 Controls for closed systems.

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. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to conclusively discern invalid or altered records.

(b) The ability to generate true copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

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

(d) Limiting system access to authorized individuals.

(e) Use of time stamped audit trails to document record changes, all write to file operations, and to independently record the date and time of operator entries and actions. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as required for the subject electronic documents and shall be available for agency review and copying.

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

(g) Use of authority checks to ensure that only those individuals who have been so authorized can use the system, electronically sign a record, access the operation or device, alter a record, or perform the operation at hand.

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

(i) Confirmation that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

(j) The establishment of, and adherence to, written policies which hold individuals accountable and liable for actions initiated under their electronic signatures, so as to deter record and signature falsification.

(k) Use of appropriate systems documentation controls including:

(i) Adequate controls over the distribution, access to, and use of documentation for system operation and maintenance.

(ii) Records revision and change control procedures to maintain an electronic audit trail that documents time-sequenced development and modification of records.

§ 11.30 Controls for open systems

.

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. 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.

§ 11.50 Signature manifestations

.

(a) Electronic records which are electronically signed shall display, in clear text, the printed name of the signer and the date and time when the electronic signature was executed.

(b) Electronic records shall clearly indicate the meaning (such as review, approval, responsibility, and authorship) associated with their attendant signatures.

§ 11.70 Signature/record binding

.

Electronic signatures and handwritten signatures executed to electronic records shall be verifiably bound to their respective electronic records to ensure that the signatures cannot be excised, copied or otherwise transferred so as to falsify another electronic record.

Subpart C--Electronic Signatures

§ 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused or reassigned to anyone else.

(b) Before an electronic signature is assigned to a person, the identity of the individual shall be verified by the assigning authority.

(c) Persons utilizing electronic signatures shall certify to the agency that their electronic signature system guarantees the authenticity, validity, and binding of any electronic signature. Persons utilizing electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is authentic, valid, and binding. The certification should be submitted to the agency district office in which territory the electronic signature system is in use.

§ 11.200 Identification mechanisms and controls.

(a) Electronic signatures which are not based upon biometric/behavioral links shall:

(1) Employ at least two distinct identification mechanisms (such as an identification code and password), each of which is contemporaneously executed at each signing;

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than it's genuine owner requires collaboration of two or more individuals.

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

§ 11.300 Controls for identification codes/passwords.

Electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each issuance of identification code and password.

(b) Ensuring that identification code/password issuances are periodically checked, recalled, or revised.

(c) Following loss management procedures to electronically deauthorize lost tokens, cards, etc., and to issue temporary or permanent replacements using suitable, rigorous controls for substitutes.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and detect and report in an emergent manner any attempts at their unauthorized use to the system security unit, and to organizational management.

(e) Initial and periodic testing of devices, such as tokens or cards, bearing the identifying information, for proper function.

Dated: August 23, 1994

William K. Hubbard
Acting Deputy Commissioner for Policy