Administration (SBA) estimates that over 3,221 firms are small businesses (i.e., have fewer than 500 employees). SBA also estimates that 504 pharmaceutical firms are small businesses with fewer than 500 employees. Of the approximately 2,204 registered blood and plasma establishments that are neither government-owned nor part of the American Red Cross, most are nonprofit establishments that are not nationally dominant and thus may be small entities as defined by the Regulatory Flexibility Act.

Not all submissions will immediately be acceptable electronically, even if the submission and the electronic record conform to the criteria set forth in this rule. A particular required submission will be acceptable in electronic form only after it has been identified to this effect in public docket 92S-0251. (The agency unit that can receive that electronic submission will also be identified in the docket.) Thus, although all small entities subject to FDA regulations are potentially affected by this rule, the rule will actually only benefit those that: (1) Are required to submit records or other documents that have been identified in the public docket as acceptable if submitted electronically, and (2) choose this method of submission, instead of traditional paper record submissions. The potential range of submissions includes such records as new drug applications, medical device premarket notifications, food additive petitions, and medicated feed applications. These, and all other required submissions, will be considered by FDA as candidates for optional electronic format.

Although the benefits of making electronic submissions to FDA will be phased in over time, as the agency accepts more submissions in electronic form, firms can, upon the rule's effective date, immediately benefit from using electronic records/signatures for records they are required to keep, but not submit to FDA. Such records include, but are not limited to: Pharmaceutical and medical device batch production records, complaint records, and food processing records.

Some small entities will be affected by this rule even if they are not among the industries regulated by FDA. Because it will increase the market demand for certain types of software (e.g., document management, signature, and encryption software) and services (e.g., digital notaries and digital signature certification authorities), this rule will benefit some small firms engaged in developing and providing those products and services.

C. Description of the Impact

For any paper record that an entity is required to keep under existing statutes or FDA regulations, FDA will now accept an electronic record instead of a paper one, as long as the electronic record conforms to the requirements of this rule. FDA will also consider an electronic signature to be equivalent to a handwritten signature if it meets the requirements of this rule. Thus, entities regulated by FDA may, if they choose, submit required records and authorizations to the agency electronically once those records have been listed in the docket as acceptable in electronic form. This action is voluntary; paper records and handwritten signatures are still fully acceptable. No entity will be required to change the way it is currently allowed to submit paper records to the agency.

1. Benefits and costs

For any firm choosing to convert to electronic recordkeeping, the direct benefits are expected to include:

(1) Improved ability for the firm to analyze trends, problems, etc., enhancing internal evaluation and quality control;

(2) Reduced data entry errors, due to automated checks;

(3) Reduced costs of storage space;

(4) Reduced shipping costs for data transmission to FDA; and

(5) More efficient FDA reviews and approvals of FDA-regulated products.

No small entity will be required to convert to electronic submissions. Furthermore, it is expected that no individual firm, or other entity, will choose the electronic option unless that firm finds that the benefits to the firm from conversion will exceed any conversion costs.

There may be some small entities that currently submit records on paper, but archive records electronically. These entities will need to ensure that their existing electronic systems conform to the requirements for electronic recordkeeping described in this rule. Once they have done so, however, they may also take advantage of all the other benefits of electronic recordkeeping. Therefore, no individual small entity is expected to experience direct costs that exceed benefits as a result of this rule.

Furthermore, because almost all of the rule's provisions reflect contemporary security measures and controls that respondents to the ANPRM identified, most firms should have to make few, if any, modifications to their systems.

For entities that do choose electronic recordkeeping, the magnitude of the costs associated with doing so will depend on several factors, such as the level of appropriate computer hardware and software already in place in a given firm, the types of conforming technologies selected, and the size and dispersion of the firm. For example, biometric signature technologies may be more expensive than nonbiometric technologies; firms that choose the former technology may encounter relatively higher costs. Large, geographically dispersed firms may need some institutional security procedures that smaller firms, with fewer persons in more geographically concentrated areas, may not need. Firms that require wholesale technology replacements in order to adopt electronic record/signature technology may face much higher costs than those that require only minor modifications (e.g., because they already have similar technology for internal security and quality control purposes). Among the firms that must undertake major changes to implement electronic recordkeeping, costs will be lower for those able to undertake these changes simultaneously with other planned computer and security upgrades. New firms entering the market may have a slight advantage in implementing technologies that conform with this rule, because the technologies and associated procedures can be put in place as part of the general startup.

2. Compliance requirements

If a small entity chooses to keep electronic records and/or make electronic submissions, it must do so in ways that conform to the requirements for electronic records and electronic signatures set forth in this rule. These requirements, described previously in section II. of this document, involve measures designed to ensure the integrity of system operations, of information stored in the system, and of the authorized signatures affixed to electronic records. The requirements apply to all small (and large) entities in all industry sectors regulated by FDA.

The agency believes that because the rule is flexible and reflects contemporary standards, firms should have no difficulty in putting in place the needed systems and controls. However, to assist firms in meeting the provisions of this rule, FDA may hold public meetings and publish more detailed guidance. Firms may contact FDA's Industry and Small Business Liaison Staff, HF-50, at 5600 Fishers Lane, Rockville, MD 20857 (301-827-3430) for more information.

3. Professional skills required

If a firm elects electronic recordkeeping and submissions, it must take steps to ensure that all persons involved in developing, maintaining, and using electronic records and electronic signature systems have the education, training, and experience to perform the tasks involved. The level of training and experience that will be required depends on the tasks that the person performs. For example, an individual whose sole involvement with electronic records is infrequent might only need sufficient training to understand and use the required procedures. On the other hand, an individual involved in developing an electronic record system for a firm wishing to convert from a paper recordkeeping system would probably need more education or training in computer systems and software design and implementation. In addition, FDA expects that such a person would also have specific on-the-job training and experience related to the particular type of records kept by that firm.

The relevant education, training, and experience of each individual involved in developing, maintaining, or using electronic records/submissions must be documented. However, no specific examinations or credentials for these individuals are required by the rule.

D. Minimizing the Burden on Small Entities

This rule includes several conditions that an electronic record or signature must meet in order to be acceptable as an alternative to a paper record or handwritten signature. These conditions are necessary to permit the agency to protect and promote the public health. For example, FDA must retain the ability to audit records to detect unauthorized modifications, simple errors, and to deter falsification. Whereas there are many scientific techniques to show changes in paper records (e.g., analysis of the paper, signs of erasures, and handwriting analysis), these methods do not apply to electronic records. For electronic records and submissions to have the same integrity as paper records, they must be developed, maintained, and used under circumstances that make it difficult for them to be inappropriately modified. Without these assurances, FDA's objective of enabling electronic records and signatures to have standing equal to paper records and handwritten signatures, and to satisfy the requirements of existing statutes and regulations, cannot be met.

Within these constraints, FDA has attempted to select alternatives that provide as much flexibility as practicable without endangering the integrity of the electronic records. The agency decided not to make the required extent and stringency of controls dependent on the type of record or transactions, so that firms can decide for themselves what level of controls are worthwhile in each case. For example, FDA chose to give firms maximum flexibility in determining: (1) The circumstances under which management would have to be notified of security problems, (2) the means by which firms achieve the required link between an electronic signature and an electronic record, (3) the circumstances under which extra security and authentication measures are warranted in open systems, (4) when to use operational system checks to ensure proper event sequencing, and (5) when to use terminal checks to ensure that data and instructions originate from a valid source.

Numerous other specific considerations were addressed in the public comments to the proposed rule. A summary of the issues raised by those comments, the agency's assessment of these issues, and any changes made in the proposed rule as a result of these comments is presented earlier in this preamble.

FDA rejected alternatives for limiting potentially acceptable electronic submissions to a particular category, and for issuing different electronic submissions standards for small and large entities. The former alternative would unnecessarily limit the potential benefits of this rule; whereas the latter alternative would threaten the integrity of electronic records and submissions from small entities.

As discussed previously in this preamble, FDA rejected comments that suggested a total of 17 additional more stringent controls that might be more expensive to implement. These include: (1) Examination and certification of individuals who perform certain important tasks, (2) exclusive use of cryptographic methods to link electronic signatures to electronic records, (3) controls for each possible combination of a two factored authentication method, (4) controls for each different type of identification card, and (5) recording in audit trails the reason why records were changed.

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, the Public Health Service Act, and under authority delegated to the Commissioner of Food and Drugs, Title 21, Chapter I of the Code of Federal Regulations is amended by adding part 11 to read as follows:

PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A—General Provisions

Subpart B—Electronic Records

Subpart C—Electronic Signatures

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

Subpart A—General Provisions

§ 11.1 Scope.

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

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after

August 20, 1997.

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

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

§ 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

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

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

§ 11.3 Definitions.

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

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

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B—Electronic Records

§ 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

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

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

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

(d) Limiting system access to authorized individuals.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

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

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

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

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

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

(k) Use of appropriate controls over systems documentation including:

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

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

§ 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to

ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

§ 11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

§ 11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Subpart C—Electronic Signatures

§ 11.100 General requirements.

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

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

§ 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

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

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

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

§ 11.300 Controls for identification codes/passwords.

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

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

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

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

Dated: March 11, 1997.

William B. Schultz,

Deputy Commissioner for Policy.

[FR Doc. 97–6833 Filed 3–20–97; 8:45 am]

BILLING CODE 4160–01–F

日本における電子記録・電子署名

- 1997年7月18日
  厚生省医薬安全局監視指導課長（医薬監第14号）：
  「医薬品並びに医療用具の製造管理及び品質管理に関する記録の磁気媒体等による保存について」
- 1997年8月13日
  厚生省医薬安全局監視指導課品質指導係事務連絡：
  「医薬品の品質管理等に関する記録への電子ファイルの利用方法に関する研究」 1995、1996年の厚生科学研究報告書
- 1997年12月18日
  日本製薬団体連合会GMP委員会（日薬連発第959号）
  加盟団体の会員メーカーから寄せられた質問に対するQ&A

要検討課題

- 適用範囲
  - GXP
  - 既存設備
- 電子署名
  - 法的な定義、原本及びリンク
- 電子記録
  - 作成中の電子記録、(原本及びリンク)
- 経過措置
  - 技術の現状
  - 社会的な現状

海外指針との比較 (1)

本指針	*21 CFR Part11*	*EU GMP Annex11*	*TGA GMP*
第1 目的	A-11.1 (a)		
第2 用語の定義	A-11.3 (a), (b)		
(1) 電子記録	A-11.3 (b) (6)		
(2) 電子媒体			
(3) 電子署名	A-11.3 (b) (7), B-11.70		
第3 適用範囲	A-11.1 (b), (c), (d) A-11.2 (b), B-11.100 (c)		

海外指針との比較 (2)

本指針	*21 CFR Part11*	*EU GMP Annex11*	*TGA GMP*
第4 利用の要件 1. 電子記録の管理			
(1) 真正性	B-11.10, B-11.30		
ア 作業者	B-11.10 (d), (g) B-11.100 (a), (b) B-11.200 (a), (b) B-11.300, (a), (b), (c) (d), (e)	8.1, 8.3 10.1, 10.2 19.1	4.5.1 4.5.2 4.5.3
イ 手順	B-11.10 (h) , (f) B-11.300 (d)	8.2	
ウ 電子署名	B-11.10 (e) B-11.50 (a), (b)	10.4	

海外指針との比較 (3)

本指針	*21 CFR Part11*	*EU GMP Annex11*	*TGA GMP*
エ 監査証跡	B-11.10 (a), (e)		
オ バックアップ	B-11.10 (b), (c)	12.1, 13.2	
(2) 見読性	B-11.10 (b)	12.1	
表示 ・ 印字	B-11.10 (b), B-11.50 (a), (b)	12.1	
(3) 保存性	B-11.10 (c)	13.2	
保存媒体	B-11.10 (b)	12.1	
(4) 変換	A-11.1(e), B-11.10 (c)	13.2	

海外指針との比較 (4)

本指針	*21 CFR Part11*	*EU GMP Annex11*	*TGA GMP*
2. 製造業者の措置	A-11.2 (a) B-11.10 (i), (j), (k)	8.4	