参考資料３

Thursday
March 20, 1997

federal register

Part II

Department of Health and Human Services

Food and Drug Administration

21 CFR Part 11

Electronic Records; Electronic Signatures; Final Rule

Electronic Submissions; Establishment of Public Docket; Notice

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

21 CFR Part 11

[Docket No. 92N-0251]

RIN 0910-AA29

Electronic Records; Electronic Signatures

AGENCY: Food and Drug Administration, HHS.

ACTION: Final rule.

SUMMARY: The Food and Drug Administration (FDA) is issuing regulations that provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, are intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health. The use of electronic records as well as their submission to FDA is voluntary. Elsewhere in this issue of the Federal Register, FDA is publishing a document providing information concerning submissions that the agency is prepared to accept electronically .

DATES: Effective August 20, 1997. Submit written comments on the information collection provisions of this final rule by May 19, 1997.

ADDRESSES: Submit written comments on the information collection provisions of this final rule to the Dockets Management Branch (HFA-305), Food and Drug Administration, 12420 Parklawn Dr., rm. 1-23, Rockville, MD 20857.

The final rule is also available electronically via Internet: http://www.fda.gov.

FOR FURTHER INFORMATION CONTACT:

Paul J. Motise, Center for Drug Evaluation and Research (HFD-325), Food and Drug Administration, 7520 Standish Pl., Rockville, MD 20855, 301-594-1089. E-mail address via Internet: Motise@CDER.FDA.GOV, or

Tom M. Chin, Division of Compliance Policy (HFC-230), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857, 301-827-0410. E-mail address via Internet: TChin@FDAEM.SSW.DHHS.GOV

SUPPLEMENTARY INFORMATION:

I. Background

In 1991, members of the pharmaceutical industry met with the agency to determine how they could accommodate paperless record systems under the current good manufacturing practice (CGMP) regulations in parts 210 and 211 (21 CFR parts 210 and 211). FDA created a Task Force on Electronic Identification/Signatures to develop a uniform approach by which the agency could accept electronic signatures and records in all program areas. In a February 24, 1992, report, a task force subgroup, the Electronic Identification/Signature Working Group, recommended publication of an advance notice of proposed rulemaking (ANPRM) to obtain public comment on the issues involved.

In the Federal Register of July 21, 1992 (57 FR 32185), FDA published the ANPRM, which stated that the agency was considering the use of electronic identification/signatures, and requested comments on a number of related topics and concerns. FDA received 53 comments on the ANPRM. In the Federal Register of August 31, 1994 (59 FR 45160), the agency published a proposed rule that incorporated many of the comments to the ANPRM, and requested that comments on the proposed regulation be submitted by November 29, 1994. A complete discussion of the options considered by FDA and other background information on the agency's policy on electronic records and electronic signatures can be found in the ANPRM and the proposed rule.

FDA received 49 comments on the proposed rule. The commenters represented a broad spectrum of interested parties: Human and veterinary pharmaceutical companies as well as biological products, medical device, and food interest groups, including 11 trade associations, 25 manufacturers, and 1 Federal agency.

II. Highlights of the Final Rule

The final rule provides criteria under which FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures. Part 11 (21 CFR part 11) applies to any paper records required by statute or agency regulations and supersedes any existing paper record requirements by providing that electronic records may be used in lieu of paper records. Electronic signatures which meet the requirements of the rule will be considered to be equivalent to full handwritten signatures, initials, and other general signings required by agency regulations.

Section 11.2 provides that records may be maintained in electronic form and electronic signatures may be used in lieu of traditional signatures. Records and signatures submitted to the agency may be presented in an electronic form provided the requirements of part 11 are met and the records have been identified in a public docket as the type of submission the agency accepts in an electronic form. Unless records are identified in this docket as appropriate for electronic submission, only paper records will be regarded as official submissions.

Section 11.3 defines terms used in part 11, including the terms: Biometrics, closed system, open system, digital signature, electronic record, electronic signature, and handwritten signature.

Section 11.10 describes controls for closed systems, systems to which access is controlled by persons responsible for the content of electronic records on that system. These controls include measures designed to ensure the integrity of system operations and information stored in the system. Such measures include: (1) Validation; (2) the ability to generate accurate and complete copies of records; (3) archival protection of records; (4) use of computer-generated, time-stamped audit trails; (5) use of appropriate controls over systems documentation; and (6) a determination that persons who develop, maintain, or use electronic records and signature systems have the education, training, and experience to perform their assigned tasks.

Section 11.10 also addresses the security of closed systems and requires that: (1) System access be limited to authorized individuals; (2) operational system checks be used to enforce permitted sequencing of steps and events as appropriate; (3) authority checks be used 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 operations; (4) device (e.g., terminal) checks be used to determine the validity of the source of data input or operation instruction; and (5) written policies be established and adhered to holding individuals accountable and responsible for actions initiated under their electronic signatures, so as to deter record and signature falsification.

Section 11.30 sets forth controls for open systems, including the controls required for closed systems in § 11.10 and additional measures such as document encryption and use of appropriate digital signature standards

to ensure record authenticity, integrity, and confidentiality.

Section 11.50 requires signature manifestations to contain information associated with the signing of electronic records. This information must include the printed name of the signer, the date and time when the signature was executed, and the meaning (such as review, approval, responsibility, and authorship) associated with the signature. In addition, this information is subject to the same controls as for electronic records and must be included in any human readable forms of the electronic record (such as electronic display or printout).

Under § 11.70, electronic signatures and handwritten signatures executed to electronic records must be linked to their respective records so that signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Under the general requirements for electronic signatures, at § 11.100, each electronic signature must be unique to one individual and must not be reused by, or reassigned to, anyone else. Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, the organization shall verify the identity of the individual.

Section 11.200 provides that electronic signatures not based on biometrics must employ at least two distinct identification components such as an identification code and password. In addition, when an individual executes a series of signings during a single period of controlled system access, the first signing must be executed using all electronic signature components and the subsequent signings must be executed using at least one component designed to be used only by that individual. When an individual executes one or more signings not performed during a single period of controlled system access, each signing must be executed using all of the electronic signature components.

Electronic signatures not based on biometrics are also required to be used only by their genuine owners and administered and executed to ensure that attempted use of an individual's electronic signature by anyone else requires the collaboration of two or more individuals. This would make it more difficult for anyone to forge an electronic signature. Electronic signatures based upon biometrics must be designed to ensure that such signatures cannot be used by anyone other than the genuine owners.

Under § 11.300, electronic signatures based upon use of identification codes in combination with passwords must employ controls to ensure security and integrity. The controls must include the following provisions: (1) The uniqueness of each combined identification code and password must be maintained in such a way that no two individuals have the same combination of identification code and password; (2) persons using identification codes and/or passwords must ensure that they are periodically recalled or revised; (3) loss management procedures must be followed to deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification codes or password information; (4) transaction safeguards must be used to prevent unauthorized use of passwords and/or identification codes, and to detect and report any attempt to misuse such codes; (5) devices that bear or generate identification codes or password information, such as tokens or cards, must be tested initially and periodically to ensure that they function properly and have not been altered in an unauthorized manner.

III. Comments on the Proposed Rule

A. General Comments

1. Many comments expressed general support for the proposed rule. Noting that the proposal's regulatory approach incorporated several suggestions submitted by industry in comments on the ANPRM, a number of comments stated that the proposal is a good example of agency and industry cooperation in resolving technical issues.

Several comments also noted that both industry and the agency can realize significant benefits by using electronic records and electronic signatures, such as increasing the speed of information exchange, cost savings from the reduced need for storage space, reduced errors, data integration/trending, product improvement, manufacturing process streamlining, improved process control, reduced vulnerability of electronic signatures to fraud and abuse, and job creation in industries involved in electronic record and electronic signature technologies.

One comment noted that, when part 11 controls are satisfied, electronic signatures and electronic records have advantages over paper systems, advantages that include: (1) Having automated databases that enable more advanced searches of information, thus obviating the need for manual searches of paper records; (2) permitting information to be viewed from multiple perspectives; (3) permitting determination of trends, patterns, and behaviors; and (4) avoiding initial and subsequent document misfiling that may result from human error.

There were several comments on the general scope and effect of proposed part 11. These comments noted that the final regulations will be viewed as a standard by other Government agencies, and may strongly influence the direction of electronic record and electronic signature technologies. One comment said that FDA's position on electronic signatures/electronic records is one of the most pressing issues for the pharmaceutical industry and has a significant impact on the industry's future competitiveness. Another comment said that the rule constitutes an important milestone along the Nation's information superhighway.

FDA believes that the extensive industry input and collaboration that went into formulating the final rule is representative of a productive partnership that will facilitate the use of advanced technologies. The agency acknowledges the potential benefits to be gained by electronic record/electronic signature systems. The agency expects that the magnitude of these benefits should significantly outweigh the costs of making these systems, through compliance with part 11, reliable, trustworthy, and compatible with FDA's responsibility to promote and protect public health. The agency is aware of the potential impact of the rule, especially regarding the need to accommodate and encourage new technologies while maintaining the agency's ability to carry out its mandate to protect public health. The agency is also aware that other Federal agencies share the same concerns and are addressing the same issues as FDA; the agency has held informal discussions with other Federal agencies and participated in several interagency groups on electronic records/electronic signatures and information technology issues. FDA looks forward to exchanging information and experience with other agencies for mutual benefit and to promote a consistent Federal policy on electronic records and signatures. The agency also notes that benefits, such as the ones listed by the comments, will help to offset any system modification costs that persons may incur to achieve compliance with part 11.

B. Regulations Versus Guidelines

2. Several comments addressed whether the agency's policy on electronic signatures and electronic records should be issued as a regulation

or recommended in a guideline. Most comments supported a regulation, citing the need for a practical and workable approach for criteria to ensure that records can be stored in electronic form and are reliable, trustworthy, secure, accurate, confidential, and authentic. One comment specifically supported a single regulation covering all FDA-regulated products to ensure consistent requirements across all product lines. Two comments asserted that the agency should only issue guidelines or "make the regulations voluntary." One of these comments said that by issuing regulations, the agency is shifting from creating tools to enhance communication (technological quality) to creating tools for enforcement (compliance quality).

The agency remains convinced, as expressed in the preamble to the proposed rule (59 FR 45160 at 45165), that a policy statement, inspection guide, or other guidance would be an inappropriate means for enunciating a comprehensive policy on electronic signatures and records. FDA has concluded that regulations are necessary to establish uniform, enforceable, baseline standards for accepting electronic signatures and records. The agency believes, however, that supplemental guidance documents would be useful to address controls in greater detail than would be appropriate for regulations. Accordingly, the agency anticipates issuing supplemental guidance as needed and will afford all interested parties the opportunity to comment on the guidance documents.

The need for regulations is underscored by several opinions expressed in the comments. For example, one comment asserted that it should be acceptable for supervisors to remove the signatures of their subordinates from signed records and replace them with their own signatures. Although the agency does not object to the use of a supervisor's signature to endorse or confirm a subordinate's actions, removal of an original signature is an action the agency views as falsification. Several comments also argued that an electronic signature should consist of only a password, that passwords need not be unique, that it is acceptable for people to use passwords associated with their personal lives (like the names of their children or their pets), and that passwords need only be changed every 2 years. FDA believes that such procedures would greatly increase the possibility that a password could be compromised and the chance that any resulting impersonation and/or falsification would continue for a long time. Therefore, an enforceable regulation describing the acceptable characteristics of an electronic signature appears necessary.

C. Flexibility and Specificity

3. Several comments addressed the flexibility and specificity of the proposed rule. The comments contended that agency acceptance of electronic records systems should not be based on any particular technology, but rather on the adequacy of the system controls under which they are created and managed. Some comments claimed that the proposed rule was overly prescriptive and that it should not specify the mechanisms to be used, but rather only require owners/users to design appropriate safeguards and validate them to reasonably ensure electronic signature integrity and authenticity. One comment commended the agency for giving industry the freedom to choose from a variety of electronic signature technologies, while another urged that the final rule be more specific in detailing software requirements for electronic records and electronic notebooks in research and testing laboratories.

The agency believes that the provisions of the final rule afford firms considerable flexibility while providing a baseline level of confidence that records maintained in accordance with the rule will be of high integrity. For example, the regulation permits a wide variety of existing and emerging electronic signature technologies, from use of identification codes in conjunction with manually entered passwords to more sophisticated biometric systems that may necessitate additional hardware and software. While requiring electronic signatures to be linked to their respective electronic records, the final rule affords flexibility in achieving that link through use of any appropriate means, including use of digital signatures and secure relational database references. The final rule accepts a wide variety of electronic record technologies, including those based on optical storage devices. In addition, as discussed in comment 40 of this document, the final rule does not establish numerical standards for levels of security or validation, thus offering firms flexibility in determining what levels are appropriate for their situations. Furthermore, while requiring operational checks, authority checks, and periodic testing of identifying devices, persons have the flexibility of conducting those controls by any suitable method. When the final rule calls for a certain control, such as periodic testing of identification tokens, persons have the option of determining the frequency.

D. Controls for Electronic Systems Compared with Paper Systems

4. Two comments stated that any controls that do not apply to paper-based document systems and handwritten signatures should not apply to electronic record and signature systems unless those controls are needed to address an identified unique risk associated with electronic record systems. One comment expressed concern that FDA was establishing a much higher standard for electronic signatures than necessary.

In attempting to establish minimum criteria to make electronic signatures and electronic records trustworthy and reliable and compatible with FDA's responsibility to promote and protect public health (e.g., by hastening the availability of new safe and effective medical products and ensuring the safety of foods), the agency has attempted to draw analogies to handwritten signatures and paper records wherever possible. In doing so, FDA has found that the analogy does not always hold because of the differences between paper and electronic systems. The agency believes some of those differences necessitate controls that will be unique to electronic technology and that must be addressed on their own merits and not evaluated on the basis of their equivalence to controls governing paper documents.

The agency found that some of the comments served to illustrate the differences between paper and electronic record technologies and the need to address controls that may not generally be found in paper record systems. For example, several comments pointed out that electronic records built upon information databases, unlike paper records, are actually transient views or representations of information that is dispersed in various parts of the database. (The agency notes that the databases themselves may be geographically dispersed but linked by networks.) The same software that generates representations of database information on a screen can also misrepresent that information, depending upon how the software is written (e.g., how a query is prepared). In addition, database elements can easily be changed at any time to misrepresent information, without evidence that a change was made, and in a manner that destroys the original information. Finally, more people have potential access to electronic record

systems than may have access to paper records.

Therefore, controls are needed to ensure that representations of database information have been generated in a manner that does not distort data or hide noncompliant or otherwise bad information, and that database elements themselves have not been altered so as to distort truth or falsify a record. Such controls include: (1) Using time-stamped audit trails of information written to the database, where such audit trails are executed objectively and automatically rather than by the person entering the information, and (2) limiting access to the database search software. Absent effective controls, it is very easy to falsify electronic records to render them indistinguishable from original, true records.

The traditional paper record, in comparison, is generally a durable unitized representation that is fixed in time and space. Information is recorded directly in a manner that does not require an intermediate means of interpretation. When an incorrect entry is made, the customary method of correcting FDA-related records is to cross out the original entry in a manner that does not obscure the prior data. Although paper records may be falsified, it is relatively difficult (in comparison to falsification of electronic records) to do so in a nondetectable manner. In the case of paper records that have been falsified, a body of evidence exists that can help prove that the records had been changed; comparable methods to detect falsification of electronic records have yet to be fully developed.

In addition, there are significant technological differences between traditional handwritten signatures (recorded on paper) and electronic signatures that also require controls unique to electronic technologies. For example, the traditional handwritten signature cannot be readily compromised by being "loaned" or "lost," whereas an electronic signature based on a password in combination with an identification code can be compromised by being "loaned" or "lost." By contrast, if one person attempts to write the handwritten signature of another person, the falsification would be difficult to execute and a long-standing body of investigational techniques would be available to detect the falsification. On the other hand, many electronic signatures are relatively easy to falsify and methods of falsification almost impossible to detect.

Accordingly, although the agency has attempted to keep controls for electronic record and electronic signatures analogous to traditional paper systems, it finds it necessary to establish certain controls specifically for electronic systems.

E. FDA Certification of Electronic Signature Systems

5. One comment requested FDA certification of what it described as a low-cost, biometric-based electronic signature system, one which uses dynamic signature verification with a parameter code recorded on magnetic stripe cards.

The agency does not anticipate the need to certify individual electronic signature products. Use of any electronic signature system that complies with the provisions of part 11 would form the basis for agency acceptance of the system regardless of what particular technology or brand is used. This approach is consistent with FDA's policy in a variety of program areas. The agency, for example, does not certify manufacturing equipment used to make drugs, medical devices, or food.

F. Biometric Electronic Signatures

6. One comment addressed the agency's statement in the proposed rule (59 FR 45160 at 45168) that the owner of a biometric/behavioral link could not lose or give it away. The comment stated that it was possible for an owner to "lend" the link for a file to be opened, as a collaborative fraudulent gesture, or to unwittingly assist a fraudulent colleague in an "emergency," a situation, the comment said, that was not unknown in the computer industry.

The agency acknowledges that such fraudulent activity is possible and that people determined to falsify records may find a means to do so despite whatever technology or preventive measures are in place. The controls in part 11 are intended to deter such actions, make it difficult to execute falsification by mishap or casual misdeed, and to help detect such alterations when they occur (see § 11.10 (introductory paragraph and especially §§ 11.10(j) and 11.200(b)).

G. Personnel Integrity

7. A few comments addressed the role of individual honesty and trust in ensuring that electronic records are reliable, trustworthy, and authentic. One comment noted that firms must rely in large measure upon the integrity of their employees. Another said that subpart C of part 11, Electronic Signatures, appears to have been written with the belief that pharmaceutical manufacturers have an incentive to falsify electronic signatures. One comment expressed concern about possible signature falsification when an employee leaves a company to work elsewhere and the employee uses the electronic signature illegally.

The agency agrees that the integrity of any electronic signature/electronic record system depends heavily upon the honesty of employees and that most persons are not motivated to falsify records. However, the agency's experience with various types of records and signature falsification demonstrates that some people do falsify information under certain circumstances. Among those circumstances are situations in which falsifications can be executed with ease and have little likelihood of detection. Part 11 is intended to minimize the opportunities for readily executing falsifications and to maximize the chances of detecting falsifications.

Concerning signature falsification by former employees, the agency would expect that upon the departure of an employee, the assigned electronic signature would be "retired" to prevent the former employee from falsely using the signature.

H. Security of Industry Electronic Records Submitted to FDA

8. Several comments expressed concern about the security and confidentiality of electronic records submitted to FDA. One suggested that submissions be limited to such read-only formats as CD-ROM with raw data for statistical manipulation provided separately on floppy diskette. One comment suggested that in light of the proposed rule, the agency should review its own internal security procedures. Another addressed electronic records that may be disclosed under the Freedom of Information Act and expressed concern regarding agency deletion of trade secrets. One comment anticipated FDA's use of open systems to access industry records (such as medical device production and control records) and suggested that such access should be restricted to closed systems.

The agency is well aware of its legal obligation to maintain the confidentiality of trade secret information in its possession, and is committed to meet that obligation regardless of the form (paper or electronic) a record takes. The procedures used to ensure confidentiality are consistent with the provisions of part 11. FDA is also examining other controls, such as use of digital signatures, to ensure submission integrity. To permit legitimate changes to be made, the agency does not believe that it is necessary to restrict submissions to those maintained in