[Federal Register: March 20, 1997 (Volume 62, Number 54)]
[Rules and Regulations]
[Page 13429-13466]

21 CFR Part 11 - Electronic Records; Electronic Signatures; Final Rule; Electronic Submissions; Establishment of Public Docket; Notice

21 CFR Part 11

[Docket No. 92N-0251]
RIN 0910-AA29

Electronic Records; Electronic Signatures

AGENCY: Food and Drug Administration, HHS.

ACTION: Final rule.

요약(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.
전자 기록서, 전자 서명, 그리고 전자 기록서의 수기 서명을 종이 기록서와 종이 문서의 수기 서명과 동등한 것으로 FDA가 인정하는 상황과 기준을 정한 규정을 발행한다. 이 규정은 FDA의 모든 프로그램 영역에 적용되며, 공중 보건의 촉진과 보호라는 FDA의 책임과 조화를 이루는 다양한 전자 기술을 사용할 수 있도록 하기 위한 것이다. 전자 기록서의 사용과 이의 FDA 제출은 자율적인 선택 사항이다. 이 연방관보에는 FDA가 전자적으로 접수할 준비가 되어 있는 제출 문서 관련 정보가 정리되어 있다.

시행 일자(DATES): Effective August 20, 1997. Submit written comments on the

information collection provisions of this final rule by May 19, 1997.
1997년 8월 20일 시행. 이 최종 규칙의 정보 수집 조항에 대한 의견서를 1997년 5월 19일까지 제출하기 바란다.

주소(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.
이 최종 규칙의 정보 수집 조항에 관한 의견서의 제출처 주소는 다음과 같다. 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.
이 최종 규칙을 인터넷을 통해서도 제공한다.

문의처(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

보충 정보(SUPPLEMENTARY INFORMATION):

I. 배경(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.

1991년에 제약 업계 대표와 FDA가 만나, 파트 210 및 211의 CGMP 규정(21 CFR 파트 210 및 211)에 부합하면서도 종이 없는 기록 시스템을 추진하는 방안에 대해 협의했다. FDA는 모든 프로그램 영역의 전자 서명과 기록서를 FDA가 인정하는 통합적인 방법을 개발하기 위하여, "전자 식별/서명 태스크포스"를 구성했다. 1992년 2월 24일자 보고서를 통해 태스크포스 산하 조직인 "전자 식별/서명 실무 그룹"은 ANPRM(advance notice of proposed rulemaking)을 발행하여 관련 이슈에 대한 의견을 수렴하자고 권고했다.

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.
1992년 7월 21일자 연방관보(57 FR 32185)를 통해, FDA는 전자 식별/서명의 사용을 검토하고 있으며 관련 주제에 대하여 의견을 구한다는 내용의 ANPRM을 발표했다. 이에 대하여 53건의 의견이 접수되었다. 이후 1994년 8월 31일자 연방관보(59 FR 45160)를 통해, FDA는 ANPRN에 대한 여러 의견을 반영해 만든 규정안을 발표하고 이에 대한 의견을 1994년 11월 29일까지 제출하도록 요청했다. FDA가 검토한 옵션별 상세 정보와 전자 기록서 및 전자 서명에 대한 기타 배경 정보를 상기 ANPRM과 규정안에서 찾아볼 수 있다.

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.
규정안과 관련하여 49건의 의견이 접수되었다. 11개 업계 단체와 25개 제조업체, 1개 연방 기구를 포함하여, 사람 의약품 및 동물 의약품, 생물학적제제, 의료기기, 식품 등 여러 분야의 다양한 관계자가 의견을 보내왔다.

II. 최종 규정의 주요 사항(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.
이 최종 규정은 FDA가 종이 기록서와 동등하다고 생각하는 전자 기록서와 전통적인 수기 서명과 동등하다고 생각하는 전자 서명에 대한 기준을 제시한다. 파트 11(21 CFR 파트 11)은 법률 또는 FDA 규정에서 요구하는 종이 기록서에 적용되며, 종이 기록서 대신 전자 기록서를 사용할 수 있도록 함으로써 기존의 종이 기록서 요구 기준을 대체한다. 이 규정의 기준에 부합하는 전자 서명은 정식 수기 서명, 이니셜, 그리고 FDA 규정에서 요구하는 기타 일반 서명과 동등한 것으로 간주된다.

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.
섹션 11.2는 기록서를 전자 형식으로 유지할 수 있으며, 전통적인 서명 대신 전자 서명을 사용할 수 있다고 규정한다. FDA에 제출하는 기록서와 서명을 전자 형식으로 할 수 있는데, 다만 파트 11의 기준이 충족되고 FDA가 전자 형식으로 인정하여 접수하는 제출 문서 유형으로 정해진 것이어야 한다. 전자 제출에 적절한 것으로 분류된 기록서가 아니라면, 종이 기록서만 공식 제출 문서로 간주된다.

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.
섹션 11.3은 "생체 인식", "폐쇄계", "개방계", "디지털 서명", "전자 기록서", "전자 서명", "수기 서명"을 포함하여, 파트 11에서 사용되는 용어의 의미를 설명한다.

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.

섹션 11.10에서는 폐쇄계의 관리 기준을 제시하는데, 폐쇄계는 시스템에 있는 전자 기록서 내용에 책임을 지는 자가 시스템 접근을 통제하는 것이다. 이때 통제를 위하여 시스템에 저장된 정보와 시스템 운영의 완전성을 보증하기 위한 대책이 필요하다. 그러한 대책에는 (1) 밸리데이션, (2) 정확하고 완벽한 기록서 사본 제작 능력, (3) 기록서 보관 및 보호, (4) 컴퓨터 생성 타임 스탬프 방식의 감사 추적 기능, (5) 시스템 문서의 적절한 관리, (6) 전자 기록서 및 서명 시스템의 개발, 유지관리 또는 사용을 맡은 자가 지정 과업을 수행하는데 필요한 교육, 훈련, 경험을 구비하고 있는지 판단하는 것이 포함된다.

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.

또한 섹션 11.10에서는 폐쇄계의 보안 부분을 다루면서, (1) 허가 받은 자만 시스템에 접근할 수 있게 제한하고, (2) 적절한 경우에 단계와 이벤트의 허용 순서를 강제하는 운영 시스템 점검 기능을 활용하며, (3) 허가 받은 자만 시스템을 사용하고 기록서에 전자적으로 서명하며 운영 또는 컴퓨터 시스템 입력 또는 출력 장치에 접근하고 기록서를 수정하며 또는 작업을 수행할 수 있도록 하기 위한 권한 점검이 있어야 하고, (4) 작업 지시 또는 데이터 입력 소스의 유효성을 판단하기 위한 장치(예, 터미널) 점검을 실시하며, (5) 기록과 서명 변조를 방지하기 위해 전자 서명에 의해 추진된 행위를 책임지는 자를 규정한 방침 문서를 제정하고 준수할 것을 요구한다.

Section 11.30 sets forth controls for open systems, including the controls required for closed systems in Sec. 11.10 and additional measures such as document

encryption and use of appropriate digital signature standards to ensure record authenticity, integrity, and confidentiality.
섹션 11.30에서는 개방계의 관리 기준을 제시하는데, 개방계의 관리에는 섹션 11.10의 폐쇄계 관리에 관한 사항과 기록 신빙성, 완전성, 기밀유지성 보증을 위하여 적절한 디지털 서명 표준의 활용과 문서 암호화 같은 추가적인 대책이 포함된다.

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).
섹션 11.50에서는 전자 기록서의 서명과 관련된 정보를 포함하는 서명 표시 기준을 제시한다. 인쇄된 서명자의 이름, 서명 일시, 그리고 서명의 의미(예, 검토, 승인, 책임, 작성)가 포함되어야 한다. 이외에도 이 정보를 전자 기록서와 동일한 수준으로 관리해야 하며, 전자 기록서의 사람이 읽을 수 있는 형식에 포함시켜야 한다(예, 전자적 디스플레이 또는 인쇄물).

Under Sec. 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.
섹션 11.70에는 서명의 잘라내기, 복사 또는 옮기기를 통해 일반적인 수단으로 전자 기록서를 변조할 수 없도록, 전자 기록서의 전자 서명 및 수기 서명을 각각의 기록서와 링크 시켜야 한다는 기준이 제시되어 있다.

Under the general requirements for electronic signatures, at Sec. 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.
섹션 11.100에는 전자 서명에 대한 일반 기준이 제시되어 있는데, 각 전자 서명은 한 개인의 고유한 것이어야 하며, 다른 사람이 다시 사용하거나 다른 사람에게 다시 할당해서는 안 된다. 개인의 전자 서명을 설정, 할당, 인증 또는 허가하기에 앞서, 그 사람의 신원을 확인해야 한다.

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.
섹션 11.200에서는 생체인식을 바탕으로 하지 않는 전자 서명은 확인 코드 및 패스워드 같이, 최소한 두 개의 뚜렷한 확인 컴포넌트를 갖춰야 한다고 규정한다. 또한 단일의 연속적인 통제 시스템 접속 기간 동안 한 사람이 일련의 서명을 하는 경우, 첫 서명은 모든 전자 서명 컴포넌트를 활용하여 실시하고 이후 서명은 그 사람만이 사용하도록 설계된 최소한 한 개의 전자 서명 컴포넌트를 사용하여 실시한다. 단일의 연속적인 통제 시스템 접속 기간 동안 수행하지 않는 1회 이상의 서명인 경우, 각 서명은 모든 전자 서명 컴포넌트를 활용하여 실시한다.

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.
또한 생체인식을 바탕으로 하지 않는 전자 서명은 본인만 사용해야 하며, 본인 이외의 다른 사람이 사용하고자 할 때는 두 명 이상의 공동 작업이 필요하도록 관리하고 운영해야 한다. 이렇게 하면 전자 서명을 위조하기가 더 어렵게 될 것이다. 생체인식 기반 전자 서명은 본인 이외의 다른 사람이 사용할 수 없도록 설계한다.

Under Sec. 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.

섹션 11.300에서는 패스워드와 조합된 확인 코드의 사용을 기반으로 하는 전자 서명을 사용할 때는, 보안성과 완전성 보장을 위한 관리 대책을 구비해야 한다고 규정하고 있다. 이러한 관리 대책의 일환으로, (1) 각 확인 코드 및 패스워드 조합의 고유성을 유지하여, 두 사람이 동일한 확인 코드 및 패스워드 조합을 갖는 일이 없도록 하고, (2) 확인 코드 및/또는 패스워드를 주기적으로 리콜 또는 수정하며, (3) 확인 코드 또는 패스워드 정보를 갖고 있거나 발생시키는 토큰, 카드, 기타 장치가 분실, 도난, 망실 또는 훼손된 경우에 무효 처리하는, 분실 관리 절차를 준수하고, (4) 패스워드 및/또는 확인 코드의 무허가 사용을 방지하고 무허가 사용 시도를 감지하여 보고하는 트랜잭션 보안 장치를 활용하며, (5) 확인 코드 또는 패스워드 정보를 갖고 있거나 발생시키는, 토큰 또는 카드 같은 장치를 처음 도입할 때 테스트하고 이후 주기적으로 테스트하여, 적절하게 기능을 발휘하며 허가 받지 않은 방식으로 변형되지 않았음을 확인한다.