VIII. 전자 기록서 – 개방계의 관리(Electronic Records--Controls for Open Systems)(Sec. 11.30)

Proposed Sec. 11.30 states that: "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." In addition, Sec. 11.30 states: * * * Such procedures and controls shall include those identified in Sec. 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.
섹션 11.30은 다음과 같이 규정하고 있다. "전자 기록서를 생성, 변형, 유지 또는 전송하는데 사용되는 개방계는, 전자 기록서의 신빙성, 완전성, 그리고 기밀유지성을 생성 지점부터 접수 지점까지 보장하도록 설계된 절차와 관리 체계를 구축해야 한다. 이와 같은 절차와 관리 체계는 11.10에 규정된 사항과 상황에 따라 기록 신빙성, 완전성, 기밀유지성을 보장하기 위한, FDA가 인정할 수 있는 확립된 디지털 서명 표준의 활용 및 문서 암호화 같은 추가적인 대책을 포함해야 한다."

94. One comment suggested that the reference to digital signature standards be deleted because the agency should not be setting standards and should not dictate how to ensure record authenticity, integrity, and confidentiality. Other comments requested clarification of the agency's expectations with regard to digital signatures: (1) The kinds that would be acceptable, (2) the mechanism for announcing which standards were acceptable (and whether that meant FDA would be certifying particular software), and (3) a definition of digital signature. One comment asserted that FDA should accept international standards for digital signatures. Some comments also requested a definition of encryption. One comment encouraged the agency to further define open systems.
디지털 서명 표준 부분을 삭제하자는 의견이 1건 있었다. FDA가 그 표준을 설정하는 것도 아니고, 기록서의 신빙성, 완전성, 기밀유지성 보장 방법을 정할 수도 없기 때문이라는 것이다. 디지털 서명과 관련하여 다음 사항을 포함해 FDA의 기대 사항을 명확히 해달라는 요청이 있었다. (1) 수용 가능한 유형, (2) 수용 가능한 표준의 발표 메커니즘(그리고 그것이 FDA가 특정 소프트웨어를 인증한다는 의미인지 여부), (3) 디지털 서명의 정의. 디지털 서명 관련 국제 표준을 FDA가 수용해야 한다는 의견이 1건 있었다. 또한 암호화의 정의를 요청한 의견도 있었다. 개방계의 의미를 더 자세히 정의할 것을 요청한 의견도 1건

있었다.

The agency advises that Sec. 11.30 requires additional controls, beyond those identified in Sec. 11.10, as needed under the circumstances, to ensure record authenticity, integrity, and confidentiality for open systems. Use of digital signatures is one measure that may be used, but is not specifically required. The agency wants to ensure that the digital signature standard used is, in fact, appropriate. Development of digital signature standards is a complex undertaking, one FDA does not expect to be performed by individual firms on an ad hoc basis, and one FDA does not now seek to perform.

섹션 11.30은 개방계의 신빙성, 완전성, 기밀유지성 보장을 위하여, 상황에 따라 섹션 11.10에 제시된 것 이상의 추가적인 관리를 요구한다. 디지털 서명의 활용은 한 가지 방안이며, 구체적으로 요구하는 것이 아니다. 활용하는 디지털 서명 표준은 적절한 것일 필요가 있다. 디지털 서명 표준의 개발은 복잡하며, 개별 업체가 수행할 성질의 일은 아니라고 보며, FDA가 추진하고자 하는 것도 아니다.

The agency is nonetheless concerned that such standards be robust and secure. Currently, the agency is aware of two such standards, the RSA (Rivest-Shamir-Adleman), and NIST's Digital Signature Standard (DSS). The DSS became Federal Information Processing Standard (FIPS) 186 on December 1, 1994. These standards are incorporated in different software programs. The agency does not seek to certify or otherwise approve of such programs, but expects people who use such programs to ensure that they are suitable for their intended use. FDA is aware that NIST provides certifications regarding mathematical conformance to the DSS core algorithms, but does not formally evaluate the broader programs that contain those algorithms. The agency has revised the final rule to clarify its intent that firms retain the flexibility to use any appropriate digital signature as an additional system control for open systems. FDA is also including a definition of digital signature under Sec. 11.3(b)(5).

그럼에도 불구하고 디지털 서명 표준은 확실하고 안전한 것이어야 한다. 현재 두 종류의 표준이 있다(RSA(Rivest-Shamir-Adleman)과 NIST의 DSS(Digital Signature Standard)). DSS는 1994년 12월 1일자로 FIPS(Federal Information Processing Standard)가 되었다. 이 표준은 다양한 소프트웨어 프로그램에 채택되었다. FDA가 그런 프로그램을 인증하거나 승인하지 않지만, 그런 프로그램을 사용하는 사람들은 목적 용도에 적합하도록 해야 할 것이다. NIST가 DSS 핵심 알고리듬의 수학적 부합과 관련하여 인증을 하고 있지만, 이 알고리듬을 포함하는 프로그램을 공식적으로 평가하고 있지는 않다.

개방계의 추가적인 시스템 관리 방법으로써 적절한 디지털 서명을 사용하는데 있어서 업체가 유연성을 발휘할 수 있다는 점을 명확히 하는 방향으로 수정했다. 또한 디지털 서명의 용어 정의를 섹션 11.3(b)(5)에 추가했다.

The agency does not believe it necessary to codify the term "encryption" because, unlike the term digital signature, it has been in general use for many years and is generally understood to mean the transforming of a writing into a secret code or cipher. The agency is aware that there are several commercially available software programs that implement both digital signatures and encryption.
"암호화"의 의미를 규정할 필요는 없다고 생각한다. 디지털 서명과 달리 이 용어는 오랫동안 보편적으로 사용되어 왔으며, 정보를 비밀 코드나 암호로 전환하는 것이라는 의미가 널리 이해되고 있기 때문이다. 디지털 서명과 암호화 모두를 구현한 소프트웨어 프로그램이 다수 시판되고 있다.

95. Two comments noted that use of digital signatures and encryption is not necessary in the context of PDMA, where access to an electronic record is limited once it is signed and stored. One of the comments suggested that proposed Sec. 11.30 be revised to clarify this point.
디지털 서명과 암호화 활용은 PDMA의 경우에 필요하지 않다는 의견이 2건 있었다. PDMA에서는 전자 기록서를 일단 서명하고 저장하면, 전자 기록서 접근이 제한되기 때문이라는 것이다. 이 부분을 명확히 하는 방향으로 섹션 11.30을 수정해야 한다는 의견이 있었다.

As discussed in comment 94 of this document, use of digital signatures and encryption would be an option when extra measures are necessary under the circumstances. In the case of PDMA records, such measures may be warranted in certain circumstances, and unnecessary in others. For example, if electronic records were to be transmitted by a firm's representative by way of a public online service to a central location, additional measures would be necessary. On the other hand, where the representative's records are hand delivered to that location, or transferred by direct connection between the representative and the central location, such additional measures to ensure record authenticity, confidentiality, and integrity may not be necessary. The agency does not believe that it is practical to revise Sec. 11.30 to elaborate on every possible situation in which additional measures would or would not be needed.
이 문서 94번 항목에서 설명한 바와 같이, 디지털 서명과 암호화의 활용은 추가 대책이

필요한 상황에서 채택하는 선택 사항이다. PDMA 기록서인 경우에는 이런 대책이 필요한 상황도 있고 필요하지 않은 상황도 있다. 예를 들어 전자 기록서를 공공 온라인 서비스를 통해 회사 담당자가 중앙 지점으로 전송한다면, 추가적인 대책이 필요할 수 있다. 반면 담당자가 기록서를 직접 갖고 가서 전달하거나 담당자와 중앙 지점 사이의 직접 접속을 통해 전송한다면, 기록서의 신빙성, 기밀유지성, 완전성 보장을 위한 추가적인 대책은 필요하지 않을 수 있다. 추가적인 대책이 필요한 모든 상황을 세세하게 제시하는 식으로 섹션 11.30을 수정하는 것은 도움이 되지 않는다고 생각한다.

96. One comment addressed encryption of submissions to FDA and asked if people making those submissions would have to give the agency the appropriate "keys" and, if so, how the agency would protect the security of such information.
FDA 제출 문서의 암호화와 관련하여, 문서를 제출하는 자가 적절한 "키"를 FDA에 제공해야 하는지, 그렇다면 FDA는 그런 정보를 어떻게 보호할 것인지 질문한 의견이 1건 있었다.

The agency intends to develop appropriate procedures regarding the exchange of "keys" attendant to use of encryption and digital signatures, and will protect those keys that must remain confidential, in the same manner as the agency currently protects trade secrets. Where the agency and a submitter agree to use a system that calls for the exchange of secret keys, FDA will work with submitters to achieve mutually agreeable procedures. The agency notes, however, that not all encryption and digital signature systems require that enabling keys be secret.
암호화 및 디지털 서명 활용에 따른 "키"의 교환과 관련하여 적절한 절차를 개발할 계획이며, 현재 영업 비밀을 보호하기 위해 적용하는 것과 동일한 방식으로 기밀로 유지되어야 할 키를 보호할 생각이다. FDA와 제출업체가 비밀 키의 교환이 요구되는 시스템 활용에 대하여 합의를 하는 경우, FDA는 제출업체와 함께 상호 합의 가능한 절차를 만들 생각이다. 하지만 모든 암호화 및 디지털 서명 시스템이 그런 키의 비밀 유지를 요구하는 것은 아니다.

97. One comment noted that proposed Sec. 11.30 does not mention availability and nonrepudiation and requested clarification of the term "point of receipt." The comment noted that, where an electronic record is received at a person's electronic mailbox (which resides on an open system), additional measures may be needed when the record is transferred to the person's own local computer because such additional transfer entails additional security risks. The comment suggested wording that would extend open system controls to the point where records are

ultimately retained.
가용성 및 부인 방지 부분이 섹션 11.30에 없다고 지적하고, "접수 지점"의 의미를 명확히 해달라고 요청한 의견이 1건 있었다. 전자 기록서를 어떤 사람의 전자 우편함(개방계에 위치)을 통해 접수한다면, 그 기록서를 그의 로컬 컴퓨터로 옮길 때 추가적인 대책이 필요할 수 있다고 지적했다. 그와 같은 추가적인 전송은 부가적인 보안 리스크를 수반하기 때문이라는 이유에서다. 기록서가 궁극적으로 보관되는 지점까지 개방계 관리를 확대하는 식으로 수정하자고 제안했다.

The agency agrees that, in the situation described by the comment, movement of the electronic record from an electronic mailbox to a person's local computer may necessitate open system controls. However, situations may vary considerably as to the ultimate point of receipt, and FDA believes proposed Sec. 11.30 offers greater flexibility in determining open system controls than revisions suggested by the comment. The agency advises that the concept of nonrepudiation is part of record authenticity and integrity, as already covered by Sec. 11.10(c). Therefore, FDA is not revising Sec. 11.30 as suggested.
이 의견에서 설명한 상황이라면, 전자 우편함에서 개인의 컴퓨터로 전자 기록서를 이동할 때 개방계 관리가 필요할 수 있다는 점에 동의한다. 그러나 궁극적인 접수 지점과 관련한 상황이 매우 다양할 수 있으며, 이 의견에서 제시한 식의 수정보다는 현재의 섹션 11.30이 개방계 관리 수준의 결정에 있어서 업체에게 더 큰 유연성을 부여하고 있다고 생각한다. 부인 방지 개념은 섹션 11.10(c)에서 이미 설명한 바와 같이 기록서 완전성과 신빙성의 한 부분이다. 그러므로 제안한 바와 같은 수정을 하지 않는다.