§ 11.2

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.

(f) This part does not apply to records required to be established or maintained by §§1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.


§ 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:


(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 de-
vices that capture the name or mark.
(9) Open system means an environ-
ment in which system access is not
controlled by persons who are respon-
sible 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 proce-
dures and controls designed to ensure
the authenticity, integrity, and, when
appropriate, the confidentiality of elec-
tronic records, and to ensure that the
signer cannot readily repudiate the
signed record as not genuine. Such pro-
cedures and controls shall include the
following:
(a) Validation of systems to ensure
accuracy, reliability, consistent in-
tended 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 pe-
riod.
(d) Limiting system access to author-
ized individuals.
(e) Use of secure, computer-gen-
erated, 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 ob-
scure previously recorded information.
Such audit trail documentation shall
be retained for a period at least as long
as that required for the subject elec-
tronic 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 com-
puter 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 expe-
rience to perform their assigned tasks.
(j) The establishment of, and adher-
ence to, written policies that hold indi-
viduals 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 dis-
tribution of, access to, and use of docu-
mentation for system operation and
maintenance.
(2) Revision and change control pro-
cedures to maintain an audit trail that
documents time-sequenced develop-
ment and modification of systems doc-
umentation.
§ 11.30 Controls for open systems.

Persons who use open systems to cre-
ate, modify, maintain, or transmit
electronic records shall employ proce-
dures and controls designed to ensure
the authenticity, integrity, and, as ap-
propriate, the confidentiality of elec-
tronic records from the point of their
creation to the point of their receipt.
Such procedures and controls shall in-
clude those identified in §11.10, as ap-
propriate, and additional measures
such as document encryption and use
of appropriate digital signature stand-
ard to ensure, as necessary under the
circumstances, record authenticity, in-
tegrity, and confidentiality.
§ 11.50 Signature manifestations.

(a) Signed electronic records shall
contain information associated with