

FDA RULES FOR ELECTRONIC RECORDS & SIGNATURES

21 CFR Part 11

Overview

The Food and Drug Administration has strict rules on using electronic records and signatures to document or track required activities when manufacturing, packaging, holding, or distributing drugs (i.e. medical gases). Meeting Part 11 requirements can be a resource intense and expensive undertaking, depending on the level of system automation being implemented. Before attempting to adopt an electronic system to track quality control functions, GAWDA members should become familiar with the FDA requirements, set out in 21 CFR Part 11 and determine whether it is worth the investment of money and resources.

Background

In March 1997, FDA issued final Part 11 regulations that provided criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed on electronic records as being equivalent to paper records and handwritten signatures executed on paper. Although the FDA intended these rules to encourage drug manufacturers to use electronic records, the requirements have had the opposite effect – Drug manufacturers including medical gas manufacturers have been slow to adopt electronic record keeping and signature technologies to avoid compliance issues with the FDA rules.

As a result of these concerns, FDA is now re-examining part 11, and anticipate initiating rulemaking to revise provisions of that regulation. Part 11 remains in effect during the re-examination period. FDA has issued guidance to describe how they intend to exercise enforcement discretion with regard to certain part 11 requirements during this re-examination.

Applicability & Scope

The rules in Part 11 apply to records in electronic form that are “created, modified, maintained, archived, retrieved, or transmitted, under any records requirements” called for under the Food, Drug, and Cosmetic Act and the Public Health Service Act. Thus, all records required to be kept to comply with current good manufacturing practices under 21 CFR Part 211 Subpart J are subject to the electronic records provisions of Part 11. FDA states that they believe that broad interpretation could lead to unnecessary controls and costs and could discourage innovation and technological advances without providing added benefit to the public health. As a result, FDA has clarified their intent to interpret the scope of Part 11 narrowly.

Under the new, narrower interpretation, when firms choose to use records in electronic format rather than paper format, Part 11 would apply. On the other hand, when firms use computers to generate paper printouts of electronic records, and when people rely on the paper records to perform their regulated activities, the merely incidental use of computers in those instances would not trigger Part 11, providing those records meet all requirements of the predicate rules. Or put another way, the electronic means used to generate paper are subject to rules for paper, not Part 11. Your actual business practices will be taken into account by FDA to determine whether you are using electronic records and if Part 11 applies.

Example: If a record must be kept per the predicate rule, and you use a computer to generate a paper printout of the electronic records, but rely on the electronic record to perform regulated activities, FDA will consider you to be using e-record rather than paper.

Electronic Records (Closed versus Open)

The regulations have different requirements for electronic records in “closed systems” (where access is controlled by persons responsible for the system content) and “open systems” (where access is not controlled by persons responsible for system content).

Closed systems that can be assessed through the Internet may be considered open systems depending on the technology and controls employed. Users of closed systems must employ procedures to ensure the authenticity, integrity and confidentiality of the electronic records. Those procedures must include:

- Validation of systems to ensure consistency, reliability, consistent intended performance and the ability to discern invalid or altered records;
- The ability to generate accurate and complete copies of records in both human readable and electronic form;
- Protection of records including limiting access to authorized individuals;
- Use of secure, computer-generated time-stamped audit trails to record operator entries and actions modifying records;
- Operational system checks to enforce permitted sequencing of steps and events;
- Use of authority checks to ensure that only authorized persons 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;
- Terminal checks to determine the validity of source data input;
- Training of persons who use, develop, and maintain the system;
- Written policies regarding use of the system; and documentation of system controls.

Users of open systems must comply with all of the above requirements for closed systems and also adopt measures such as document encryption and use of appropriate digital signal standards to ensure record authenticity, integrity and confidentiality.

Electronic Signatures

Signed electronic records must contain information associated with the signing to indicate the printed name of the signer, date and time of the signature, and effect (review, approval, etc.) of the signature. Electronic signatures and handwritten signatures executed to electronic records must be linked to their respective electronic records to ensure that the signatures cannot be erased, copied or transferred to falsify a record. A company must notify the FDA of its intent to use electronic signatures as legally binding instruments before implementing such a system. There are also a number of specific requirements to ensure the authenticity of electronic signatures. Electronic signatures must be based on biometrics or employ two distinct identification components such as an identification code and password. Electronic signatures based on biometrics must be designed to ensure that they cannot be used by anyone other than their genuine owners, and electronic signatures based on identification codes and passwords must employ controls to ensure their security and integrity.

Legacy Systems

FDA intends to exercise enforcement discretion and will not normally take regulatory action to enforce Part 11 regarding existing or legacy systems operational before August 20, 1997, the effective date of Part 11, while they re-examining Part 11, provided all of the following criteria are met for a specific system:

- The system was operational before the effective date.
- The system met all applicable predicate rule requirements before the effective date.
- The system currently meets all applicable predicate rule requirements.
- You have documented evidence and justification that the system is fit for its intended use.

If a system has been changed since August 20, 1997, and if the changes would prevent the system from meeting predicate rule requirements, Part 11 controls should be applied.

Approach to Specific Part 11 Requirements

FDA recommends for the specific areas below that the firm base their approach on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity.

Validation – decision to validate and extent of validation, should take into account the impact the system might have on the accuracy, reliability, integrity, availability, and authenticity of required records & signatures. For instance, validation would not be important for a word processor used only to generate SOP's.

Audit Trail – it is important to have audit trails or other physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the records, as well as ensuring that changes to records do not obscure previous entries. Audit trails can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal operations.

Copies of Records – Firms must provide an investigator with reasonable and useful access to records, held in common portable formats. If you have the ability to search, sort, or trend part 11 records, copies given to the Agency should provide the same capability if it is reasonable and technically feasible.

Record Retention – requires protection of the records to enable their accurate and ready retrieval throughout the records retention period. Archived electronic records must preserve their content and meaning.

As you can see, these requirements impose a significant administrative burden on the use of electronic records and signatures. GAWDA members should review their medical gas record systems to ensure they comply in all respects with Part 11 or else switch to a paper system. Typical areas where members may have exposures to non-compliance of Part 11 requirements are:

- Employee training records kept and updated on a computer file
- Analyzer results stored on electronic media
- SOP manuals that are maintained and distributed in electronic format
- Computer systems used in the manufacture of medical gases that do not have appropriate security measures implemented to control access, including unique individual user names and regular changes of passwords.
- Distribution records of medical gases that are stored on electronic media

Many equipment and technology vendors are now selling systems that are, or can be made, Part 11 compliant.

GAWDA members using, or contemplating using, electronic record-keeping systems in their facility are advised to consult with B&R Compliance Associates – GAWDA Medical Gases Consultant – to discuss the latest compliance strategies for Part 11 compliance.

Copies of applicable regulations and guidance documents can be found following this page.

Guidance for Industry

Part 11, Electronic Records; Electronic Signatures — Scope and Application

Division of Drug Information, HFD-240
Center for Drug Evaluation and Research (CDER)
(Tel) 301-827-4573

<http://www.fda.gov/cder/guidance/index.htm>

or

Office of Communication, Training and
Manufacturers Assistance, HFM-40
Center for Biologics Evaluation and Research (CBER)
<http://www.fda.gov/cber/guidelines.htm>

Phone: the Voice Information System at 800-835-4709 or 301-827-1800

or

Communications Staff (HFV-12),
Center for Veterinary Medicine (CVM)
(Tel) 301-594-1755

<http://www.fda.gov/cvm/guidance/guidance.html>

or

Division of Small Manufacturers Assistance (HFZ-220)

<http://www.fda.gov/cdrh/ggpmain.html>

Manufacturers Assistance Phone Number: 800.638.2041 or 301.443.6597

Intern't'l Staff Phone: 301.827.3993

or

Center for Food Safety and Applied Nutrition (CFSAN)

<http://www.cfsan.fda.gov/~dms/guidance.html>

**U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Applied Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)**

**August 2003
Pharmaceutical CGMPs**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	BACKGROUND	2
III.	DISCUSSION	3
	A. Overall Approach to Part 11 Requirements.....	3
	B. Details of Approach – Scope of Part 11	4
	1. Narrow Interpretation of Scope	4..
	2. Definition of Part 11 Records	5
	C. Approach to Specific Part 11 Requirements	6
	1. Validation.....	6
	2. Audit Trail.....	6
	3. Legacy Systems	7
	4. Copies of Records	7
	5. Record Retention.....	8
IV.	REFERENCES.....	9

1 **Guidance for Industry¹**
2 **Part 11, Electronic Records; Electronic Signatures —**
3 **Scope and Application**
4
5

6 This guidance represents the Food and Drug Administration's (FDA's) current thinking on this topic. It
7 does not create or confer any rights for or on any person and does not operate to bind FDA or the public.
8 You can use an alternative approach if the approach satisfies the requirements of the applicable statutes
9 and regulations. If you want to discuss an alternative approach, contact the FDA staff responsible for
10 implementing this guidance. If you cannot identify appropriate FDA staff, call the appropriate
11 number listed on the title page of this guidance.
12
13

14
15
16 **I. INTRODUCTION**
17

18 This guidance is intended to describe the Food and Drug Administration's (FDA's) current
19 thinking regarding the scope and application of part 11 of Title 21 of the Code of Federal
20 Regulations; Electronic Records; Electronic Signatures (21 CFR Part 11).
21

22 This document provides guidance to persons who, in fulfillment of a requirement in a statute or
23 another part of FDA's regulations to maintain records or submit information to FDA, have
24 chosen to maintain the records or submit electronic information electronically and, as a result,
25 have become subject to part 11. Part 11 applies to records in electronic form that are created,
26 modified, maintained, archived, retrieved, transmitted under any records requirements set
27 forth in Agency regulations. Part 11 also applies to electronic records submitted to the Agency
28 under the Federal Food, Drug, and Cosmetic Act (the FDCA) and the Public Health Service Act (the
29 PHS Act), even if such records are not specifically identified in Agency regulations (§ 11.1).
30 The underlying requirements set forth in the FDCA, PHS Act, and FDA regulations (other than part
31 11) are referred to in this guidance document as predicate rules.
32

¹ This guidance has been prepared by the Office of Compliance in the Center for Drug Evaluation and Research (CDER) in consultation with the other Agency centers and the Office of Regulatory Affairs at the Food and Drug Administration.

² 62 FR 13430

³ These requirements include, for example, certain provisions of the Current Good Manufacturing Practice regulations (21 CFR Part 211), the Quality System regulation (21 CFR Part 820), and the Good Laboratory Practice for Nonclinical Laboratory Studies regulations (21 CFR Part 58).

Contains Nonbinding Recommendations

33 As an outgrowth of its current good manufacturing practice (CGMP) initiative for human and
34 animal drugs and biologics,⁴ FDA is re-examining part 11 as it applies to all FDA regulated
35 products. We anticipate initiating rulemaking to change part 11 as a result of that re-
36 examination. This guidance explains that we will narrowly interpret the scope of part 11. While
37 the re-examination of part 11 is under way, we intend to exercise enforcement discretion with
38 respect to certain part 11 requirements. We do not intend to take enforcement action to
39 enforce compliance with the location, audit trail, record retention, and record copying
40 requirements of part 11 as explained in this guidance. However, records must still be maintained
41 or submitted in accordance with the underlying predicate rules, and the Agency can take
42 regulatory action for noncompliance with such predicate rules.

43
44 In addition, we intend to exercise enforcement discretion and do not intend to take (or
45 recommend) action to enforce any part 11 requirements with regard to systems that were
46 operational before August 20, 1997, the effective date of part 11 (commonly known as legacy
47 systems) under the circumstances described in section III.C.3 of this guidance.

48
49 Note that part 11 remains in effect and that this exercise of enforcement discretion applies only
50 as identified in this guidance.

51
52 FDA's guidance documents, including this guide, do not establish legally enforceable
53 responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should
54 be viewed only as recommendations, unless specific regulatory or statutory requirements are
55 cited. The use of the word "should" in Agency guidances means that something is suggested or
56 recommended, but not required.

57 58 59 **II. BACKGROUND**

60
61 In March of 1997, FDA issued final part 11 regulations that provide criteria for acceptance by
62 FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten
63 signatures executed to electronic records as equivalent to paper records and handwritten
64 signatures executed on paper. These regulations, which apply to all FDA program areas, were
65 intended to permit the widest possible use of electronic technology, compatible with FDA's
66 responsibility to protect the public health.

67
68 After part 11 became effective in August 1997, significant discussions ensued among industry,
69 contractors, and the Agency concerning the interpretation and implementation of the regulations.
70 FDA has (1) spoken about part 11 at many conferences and met numerous times with an industry
71 coalition and other interested parties in an effort to hear more about potential part 11 issues; (2)
72 published a compliance policy guide, CPG 7153.17: Enforcement Policy: 21 CFR Part 11;
73 Electronic Records; Electronic Signatures; and (3) published numerous draft guidance
74 documents including the following:

⁴ See Pharmaceutical CGMPs for the 21st Century: A Risk-Based Approach; A Science and Risk-Based Approach to Product Quality Regulation Incorporating an Integrated Quality Systems Approach
www.fda.gov/oc/guidance/gmp.html.

Contains Nonbinding Recommendations

- 75
- 76 x 21 CFR Part 11; Electronic Records; Electronic Signatures, Validation
- 77 x 21 CFR Part 11; Electronic Records; Electronic Signatures, Glossary of Terms
- 78 x 21 CFR Part 11; Electronic Records; Electronic Signatures, Time Stamps
- 79 x 21 CFR Part 11; Electronic Records; Electronic Signatures, Maintenance of Electronic
- 80 Records
- 81 x 21 CFR Part 11; Electronic Records; Electronic Signatures, Electronic Copies of
- 82 Electronic Records

83

84 Throughout all of these communications, concerns have been raised that some interpretations of

85 the part 11 requirements would (1) unnecessarily restrict the use of electronic technology in a

86 manner that is inconsistent with FDA's stated intent in issuing the rule, (2) significantly increase

87 the costs of compliance to an extent that was not contemplated at the time the rule was drafted,

88 and (3) discourage innovation and technological advances without providing a significant public

89 health benefit. These concerns have been raised particularly in the areas of part 11 requirements

90 for validation, audit trails, record retention, record copying, and legacy systems.

91

92 As a result of these concerns, we decided to review the part 11 documents and related issues,

93 particularly in light of the Agency's CGMP initiative. In the Federal Register of February 4,

94 2003 (68 FR 5645), we announced the withdrawal of the draft guidance for industry, 21 CFR

95 Part 11; Electronic Records; Electronic Signatures, Electronic Copies of Electronic Records

96 We had decided we wanted to minimize industry time spent reviewing and commenting on the

97 draft guidance when that draft guidance may no longer represent our approach under the CGMP

98 initiative. Then, in the Federal Register of February 25, 2003 (68 FR 8775), we announced the

99 withdrawal of the part 11 draft guidance documents on validation, glossary of terms, time

100 stamps,⁵ maintenance of electronic records, and CPG 7153.17. We received valuable public

101 comments on these draft guidances, and we placed that information to help with future

102 decision-making with respect to part 11. We do not intend to re-issue these draft guidance

103 documents or the CPG.

104

105 We are now re-examining part 11, and we anticipate rulemaking to revise provisions of

106 that regulation. To avoid unnecessary resource expenditures to comply with part 11

107 requirements, we are issuing this guidance to describe how we intend to exercise enforcement

108 discretion with regard to certain part 11 requirements during the re-examination of part 11. As

109 mentioned previously, part 11 remains in effect during this re-examination period.

110

111

112 **III. DISCUSSION**

113

114 **A. Overall Approach to Part 11 Requirements**

115

⁵ Although we withdrew the draft guidance on time stamps, our current thinking has not changed in that when using time stamps for systems that span different time zones, we do not expect you to record the signer's local time. When using time stamps, they should be implemented with a clear understanding of the time zone reference used. In such instances, system documentation should explain time zone references as well as zone acronyms or other naming conventions.

Contains Nonbinding Recommendations

116 As described in more detail below, the approach outlined in this guidance is based on three main
117 elements:

- 118
- 119 x Part 11 will be interpreted narrowly; we are now clarifying that fewer records will be
120 considered subject to part 11.
 - 121 x For those records that remain subject to part 11, we intend to exercise enforcement
122 discretion with regard to part 11 requirements for validation, audit trails, record retention,
123 and record copying in the manner described in this guidance and with regard to all part 11
124 requirements for systems that were operational before the effective date of part 11 (also
125 known as legacy systems).
 - 126 x We will enforce all predicate rule requirements, including predicate rule record and
127 recordkeeping requirements.

128 It is important to note that FDA's exercise of enforcement discretion as described in this
129 guidance is limited to specified part 11 requirements (setting aside legacy systems, as to which
130 the extent of enforcement discretion, under certain circumstances, will be more broad). We
131 intend to enforce all other provisions of part 11 including, but not limited to, certain controls for
132 closed systems in § 11.10. For example, we intend to enforce provisions related to the following
133 controls and requirements:

- 134
- 135 x limiting system access to authorized individuals
 - 136 x use of operational system checks
 - 137 x use of authority checks
 - 138 x use of device checks
 - 139 x determination that persons who develop, train, or use electronic systems have the
140 education, training, and experience to perform their assigned tasks
 - 141 x establishment of and adherence to written policies that hold individuals accountable for
142 actions initiated under their electronic signatures
 - 143 x appropriate controls over systems documentation
 - 144 x controls for open systems corresponding to controls for closed systems bulleted above (§
145 11.30)
 - 146 x requirements related to electronic signatures (e.g., §§ 11.50, 11.70, 11.100, 11.200, and
147 11.300)

148

149 We expect continued compliance with these provisions, and we will continue to enforce them.
150 Furthermore, persons must comply with applicable predicate rules, and records that are required
151 to be maintained or submitted must remain secure and reliable in accordance with the predicate
152 rules.

153 **B. Details of Approach – Scope of Part 11**

154 **1. Narrow Interpretation of Scope**

155

156 We understand that there is some confusion about the scope of part 11. Some have understood
157 the scope of part 11 to be very broad. We believe some of those broad interpretations could

Contains Nonbinding Recommendations

160 lead to unnecessary controls and costs that could discourage innovation and technological
161 advances without providing additional benefit to the public health. As a result, we want to clarify
162 that the Agency intends to interpret the scope of part 11 narrowly.

163
164 Under the narrow interpretation of the scope of part 11, with respect to records required to be
165 maintained under predicate rules or submitted to FDA, when persons choose to use records in
166 electronic format in place of paper format, part 11 would apply. On the other hand, when
167 persons use computers to generate paper printouts of electronic records and those paper records
168 meet all the requirements of the applicable predicate rules and persons rely on the paper records
169 to perform their regulated activities, FDA would generally not consider persons to be "using
170 electronic records in lieu of paper records" under §§ 11.2(a) and 11.2(b). In these instances, the
171 use of computer systems in the generation of paper records would not trigger part 11.

172 173 2. Definition of Part 11 Records

174
175 Under this narrow interpretation, FDA considers part 11 to be applicable to the following records
176 or signatures in electronic format (part 11 records or signatures):

- 177
178 x Records that are required to be maintained under predicate requirements and that are
179 maintained in electronic format in place of paper format. On the other hand, records (and
180 any associated signatures) that are not required to be maintained under predicate rules, but
181 that are nonetheless maintained in electronic format, are not part 11 records.

182 We recommend that you determine, based on predicate rules, whether specific records
183 are part 11 records. We recommend that you document such decisions.

- 184
185 x Records that are required to be maintained under predicate rules, that are maintained in
186 electronic format in addition to paper format, and that are relied on to perform regulated
187 activities

188 In some cases, actual business practices may dictate whether you use electronic
189 records instead of paper records under § 11.2(a). For example, if a record is required to
190 be maintained under a predicate rule and you use a computer to generate a paper printout
191 of the electronic record, but you nonetheless rely on the electronic record to perform
192 regulated activities, the Agency may consider you to be using the electronic record
193 instead of the paper record. That is, the Agency may take your business practices into
194 account in determining whether part 11 applies.

195 Accordingly, we recommend that, for each record required to be maintained under
196 predicate rules, you determine in advance whether you plan to rely on the electronic
197 record or paper record to perform regulated activities. We recommend that you
198 document this decision (e.g., in a Standard Operating Procedure (SOP), or specification
199 document).

- 200 x Records submitted to FDA, under predicate rules (even if such records are not
201 specifically identified in Agency regulation) in electronic format (assuming the records
202 have been identified in docket number 9251 as the types of submissions the Agency
203 accepts in electronic format). However, a record that is not itself submitted, but is used

Contains Nonbinding Recommendations

204 in generating a submission, is not a part of a record unless it is otherwise required to be
205 maintained under a predicate rule and is maintained in electronic format.

206 x Electronic signatures that are intended to be the equivalent of handwritten signatures,
207 initials, and other general signs required by predicate rule Part 11 signatures include
208 electronic signatures that are used, for example, to document the fact that certain events
209 or actions occurred in accordance with the predicate rule (e.g., approved, reviewed, and
210 verified).

211 C. Approach to Specific Part 11 Requirements

212 1. Validation

213
214
215
216 The Agency intends to exercise enforcement discretion regarding specific part 11 requirements
217 for validation of computerized systems (§ 11.10(a) and corresponding requirements in § 11.30).
218 Although persons must still comply with all applicable predicate rule requirements for validation
219 (e.g., 21 CFR 820.70(i)), this guidance should not be used to impose any additional requirements
220 for validation.

221
222 We suggest that your decision to validate computerized systems, and the extent of the validation,
223 take into account the impact the systems have on your ability to meet predicate rule
224 requirements. You should also consider the impact those systems might have on the accuracy,
225 reliability, integrity, availability, and authenticity of required records and signatures. Even if
226 there is no predicate rule requirement to validate a system, in some instances it may still be
227 important to validate the system.

228
229 We recommend that you base your approach on a justified and documented risk assessment and
230 a determination of the potential of the system to affect product quality and safety, and record
231 integrity. For instance, validation would not be important for a word processor used only to
232 generate SOPs.

233
234 For further guidance on validation of computerized systems, see FDA's guidance for industry
235 and FDA staff General Principles of Software Validation and also industry guidance such as the
236 GAMP 4 Guide (See References).

237 2. Audit Trail

238
239
240 The Agency intends to exercise enforcement discretion regarding specific part 11 requirements
241 related to computer-generated, time-stamped audit trails (§ 11.10 (e), (k)(2) and any
242 corresponding requirement in § 11.30). Persons must comply with all applicable predicate
243 rule requirements related to documentation, for example, date (e.g., § 58.130(e)), time, or
244 sequencing of events, as well as any requirements for ensuring that changes to records do not
245 obscure previous entries.

246
247 Even if there are no predicate rule requirements to document, for example, date, time, or
248 sequence of events in a particular instance, it may nonetheless be important to have audit trails or
249 other physical, logical, or procedural security measures in place to ensure the trustworthiness and

Contains Nonbinding Recommendations

250 reliability of the records⁶. We recommend that you base your decision on whether to apply audit
251 trails, or other appropriate measures, on the need to comply with predicate rule requirements, a
252 justified and documented risk assessment, and determination of the potential effect on product
253 quality and safety and record integrity. We suggest that you apply appropriate controls based on
254 such an assessment. Audit trails can be equally appropriate when users are expected to
255 create, modify, or delete regular records during normal operation.

257 3. Legacy Systems⁷

258
259 The Agency intends to exercise enforcement discretion with respect to all part 11 requirements
260 for systems that otherwise were operational prior to August 20, 1997, the effective date of part
261 11, under the circumstances specified below.

262
263 This means that the Agency does not intend to take enforcement action to enforce compliance
264 with any part 11 requirements if all the following criteria are met for a specific system:

- 265
- 266 x The system was operational before the effective date.
- 267 x The system met all applicable predicate requirements before the effective date.
- 268 x The system currently meets all applicable predicate rule requirements.
- 269 x You have documented evidence and justification that the system is fit for its intended use
270 (including having an acceptable level of record security and integrity, if applicable).

271
272 If a system has been changed since August 1997, and if the change would prevent the
273 system from meeting predicate requirements, Part 11 controls should be applied to Part 11
274 records and signatures pursuant to the enforcement policy expressed in this guidance.

276 4. Copies of Records

277
278 The Agency intends to exercise enforcement discretion with regard to specific part 11
279 requirements for generating copies of records (§ 11.10 (b) and any corresponding requirement in
280 § 11.30). You should provide an investigator with reasonable and useful access to records during
281 an inspection. All records held by you are subject to inspection in accordance with predicate
282 rules (e.g., §§ 211.180(c), (d), and 108.35(c)(3)(ii)).

283
284 We recommend that you supply copies of electronic records by:

- 285
- 286 x Producing copies of records held in common portable formats when records are
287 maintained in these formats
- 288 x Using established automated conversion/export methods, where available, to make
289 copies in a more common format (examples of such formats include, but are not limited
290 to, PDF, XML, or SGML)

⁶ Various guidance documents on information security are available (see References).

⁷ In this guidance document, we use the term legacy system to describe systems already in operation before the effective date of part 11.

Contains Nonbinding Recommendations

291 In each case, we recommend that the copying process used produces copies that preserve the
292 content and meaning of the record. If you have the ability to search, sort, or trend part 11
293 records, copies given to the Agency should provide the same ability if it is reasonable and
294 technically feasible. You should allow inspection, review, and copying of records in a human
295 readable form at your site using your hardware and following your established procedures and
296 techniques for accessing records.

297 298 5. Record Retention

299
300 The Agency intends to exercise enforcement discretion with regard to the part 11 requirements
301 for the protection of records to enable the accurate and ready retrieval throughout the records
302 retention period (§ 11.10 (c) and any corresponding requirements in 11.30). Persons must still
303 comply with all applicable predicate rule requirements for record retention and availability (e.g.,
304 §§ 211.180(c),(d), 108.25(g), and 108.35(h)).

305
306 We suggest that your decision on how to retain records be based on predicate rule
307 requirements and that you base your decision on a justified and documented risk assessment and
308 a determination of the value of the records over time.

309
310 FDA does not intend to object if you decide to have required records in electronic format to
311 nonelectronic media such as microfilm, microfiche, or paper, or to a standard electronic file
312 format (examples of such formats include, but are not limited to, PDF, XML, or SGML).
313 Persons must still comply with all predicate rule requirements, and the records themselves and
314 any copies of the required records should preserve their content and meaning. As long as
315 predicate rule requirements are fully satisfied and the content and meaning of the records are
316 preserved and archived, you can delete the electronic version of the records. In addition, paper
317 and electronic record and signature components can co-exist (i.e., a hybrid situation) as long as
318 predicate rule requirements are met and the content and meaning of those records are preserved.

⁸ Examples of hybrid situations include combinations of paper records (or other nonelectronic media) and electronic records, paper records and electronic signatures and handwritten signatures executed to electronic records.

319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352

IV. REFERENCES

Food and Drug Administration References

1. Glossary of Computerized System and Software Development Terminology (Division of Field Investigations, Office of Regional Operations, Office of Regulatory Affairs, FDA 1995) (http://www.fda.gov/ora/inspect_ref/igs/gloss.html)
2. General Principles of Software Validation: Final Guidance for Industry and FDA Staff (FDA, Center for Devices and Radiological Health, Center for Biologics Evaluation and Research, 2002) (<http://www.fda.gov/cdrh/comp/guidance/938.html>)
3. Guidance for Industry, FDA Reviewers, and Compliance on Off-The-Shelf Software Use in Medical Devices (FDA, Center for Devices and Radiological Health, 1999) (<http://www.fda.gov/cdrh/ode/guidance/585.html>)
4. Pharmaceutical CGMPs for the 21st Century: A Risk-Based Approach; A Science and Risk-Based Approach to Product Quality Regulation Incorporating an Integrated Quality Systems Approach (FDA 2002) (<http://www.fda.gov/oc/guidance/gmp.html>)

Industry References

1. The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems, GAMP: ISPE/GAMP Forum, 2001) (<http://www.ispe.org/gamp/>)
2. ISO/IEC 17799:2000 (BS 7799:2000) Information technology – Code of practice for information security management (ISO/IEC, 2000)
3. ISO 14971:2002 Medical Devices- Application of risk management to medical devices (ISO, 2001)

Proposed Part 11

Part 11 - Electronic Records; Electronic Signatures

Subpart A- General Provisions

Sec.

- 11.1 Scope.
- 11.2 Implementation.
- 11.3 Definitions.

Subpart B - Electronic Records

- 11.10 Controls for closed systems.
- 11.30 Controls for open systems.
- 11.50 Signature manifestations.
- 11.70 Signature/record binding.

Subpart C - Electronic Signatures

- 11.100 General requirements.
- 11.200 Identification mechanisms and controls.
- 11.300 Controls for identification codes/passwords.

Authority: Secs. 201-902 of the Federal Food, Drug, and Cosmetic Act. 52 Stat. 1040 et seq., as amended (21 U.S.C. 301-392).

Subpart A--General Provisions

§ 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the Food and Drug Administration 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.

Final Part 11

Part 11 - Electronic Records; Electronic Signatures

Subpart A- General Provisions

Sec.

- 11.1 Scope.
- 11.2 Implementation.
- 11.3 Definitions.

Subpart B - Electronic Records

- 11.10 Controls for closed systems.
- 11.30 Controls for open systems.
- 11.50 Signature manifestations.
- 11.70 Signature/record linking.

Subpart C - Electronic Signatures

- 11.100 General requirements.
- 11.200 Electronic signature components and controls.
- 11.300 Controls for identification codes/passwords.

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.

Proposed Part 11

(b) These regulations apply to records in electronic form that are created, modified, maintained, or transmitted, pursuant to any records requirements set forth in chapter I of this title.

(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 throughout this chapter, unless specifically exempted by regulation that is effective on or after the effective date of this part.

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

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

§ 11.2 Implementation.

(a) For records required by chapter I of this title to be maintained, but not submitted to the agency, persons may use electronic records/signatures in lieu of paper records/conventional 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/signatures in lieu of paper records/conventional signatures, in whole or in part, provided that:

Final Part 11

(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,

Proposed Part 11

- (1) The requirements of this part are met; and
- (2) The document or parts(s) of a document to be submitted has/have been identified in public docket (docket number to be determined) 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 format without paper records and to which specific receiving unit(s) of the agency (e.g., specific center, office, division, branch) 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 should consult with the intended agency receiving unit for details on how and if 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. 201-902, 52 Stat. 1040 et seq., as amended (21 U.S.C. 301-392)).

(2) Agency means the Food and Drug Administration.

(3) Biometric/behavioral links means a method of verifying a person's identity based on measurement of the person's physical feature(s) or repeatable action(s).

Final Part 11

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. 301-393)).

(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.

Proposed Part 11

(4) Closed system means an environment in which there is communication among multiple persons, where system access is restricted to people who are part of the organization that operates the system.

(5) Electronic record means a document or writing comprised of any combination of text, graphic representation, data, audio information, or video information, that is created, modified, maintained, or transmitted in digital form by a computer or related system.

(6) Electronic signature means the entry in the form of a magnetic impulse or other form of computer data compilation of any symbol or series of symbols, executed, adopted or authorized by a person to be the legally binding equivalent of the person's handwritten signature.

(7) Handwritten signature means the name of an individual, handwritten in script by that individual, 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. However, the scripted name, while conventionally applied to paper, may also be applied to other devices which capture the written name.

(8) Open system means an environment in which there is electronic communication among multiple persons, where system access extends to people who are not part of the organization that operates the system.

Final Part 11

(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.

Proposed Part 11

Subpart B--Electronic Records

§ 11.10 Controls for closed systems.

Closed 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, 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 conclusively discern invalid or altered records.
- (b) The ability to generate true 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 time stamped audit trails to document record changes, all write to file operations, and to independently record the date and time of operator entries and actions. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as required for the subject electronic documents and shall be available for agency review and copying.
- (f) Use of operational checks to enforce permitted sequencing of events, as appropriate.

Final Part 11

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.

Proposed Part 11

(g) Use of authority checks to ensure that only those individuals who have been so authorized can use the system, electronically sign a record, access the operation or device, alter a record, or perform the operation at hand.

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

(i) Confirmation 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 which hold individuals accountable and liable for actions initiated under their electronic signatures, so as to deter record and signature falsification.

(k) Use of appropriate systems documentation controls including:

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

(ii) Records revision and change control procedures to maintain an electronic audit trail that documents time-sequenced development and modification of records.

§ 11.30 Controls for open systems

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. Such procedures and controls shall include those identified in § 11.10, as appropriate, and such additional measures as document encryption and use of established digital

Final Part 11

(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 such additional measures as document encryption and use of appropriate

Proposed Part 11

signature standards acceptable to the agency, to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

§ 11.50 Signature manifestations

(a) Electronic records which are electronically signed shall display, in clear text, the printed name of the signer and the date and time when the electronic signature was executed.

(b) Electronic records shall clearly indicate the meaning (such as review, approval, responsibility, and authorship) associated with their attendant signatures.

§ 11.70 Signature/record binding

Electronic signatures and handwritten signatures executed to electronic records shall be verifiably bound to their respective electronic records to ensure that the signatures cannot be excised, copied or otherwise transferred so as to falsify another electronic record.

Subpart C--Electronic Signatures

§ 11.100 General requirements.

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

Final Part 11

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 so as 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.

Proposed Part 11

(b) Before an electronic signature is assigned to a person, the identity of the individual shall be verified by the assigning authority.

(c) Persons utilizing electronic signatures shall certify to the agency that their electronic signature system guarantees the authenticity, validity, and binding of any electronic signature. Persons utilizing electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is authentic, valid, and binding. The certification should be submitted to the agency district office in which territory the electronic signature system is in use.

§ 11.200 Identification mechanisms and controls.

(a) Electronic signatures which are not based upon biometric/behavioral links shall:

(1) Employ at least two distinct identification mechanisms (such as an identification code and password), each of which is contemporaneously executed at each signing;

Final Part 11

(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.

Proposed Part 11

(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 biometric/behavioral links shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

§ 11.300 Controls for identification codes/passwords.

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 issuance of identification code and password.

(b) Ensuring that identification code/password issuances are periodically checked, recalled, or revised.

(c) Following loss management procedures to electronically deauthorize lost tokens, cards, etc., and to issue temporary or permanent replacements using suitable, rigorous controls for substitutes.

Final Part 11

(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.

Proposed Part 11

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

(e) Initial and periodic testing of devices, such as tokens or cards, bearing the identifying information, for proper function.

Final Part 11

(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.