

Guidance for Industry Computerized Systems Used in Clinical Trials

DRAFT GUIDANCE — ERRATUM

On line 563 of this draft guidance, reference is made to Compliance Policy Guide (CPG) # 7130.13. This is incorrect. The CPG number should be 7150.13.

**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 Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)**

**September 2004
Compliance**

Revision 1

Guidance for Industry Computerized Systems Used in Clinical Trials

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Comments and suggestions regarding this draft document should be submitted within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. All comments should be identified with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions regarding this draft document contact Patricia M. Beers Block 301-827-3340.

**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 Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)**

**September 2004
Compliance**

Revision 1

Contains Nonbinding Recommendations

Draft — Not for Implementation

Guidance for Industry Computerized Systems Used in Clinical Trials

Additional copies are available at:

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

or

<http://www.fda.gov/cber/guidelines.htm>

or

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

or

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

or

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

or

http://www.fda.gov/ora/compliance_ref/bimo

or

<http://www.fda.gov/oc/gcp>

**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 Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)**

**September 2004
Compliance**

Revision 1

Contains Nonbinding Recommendations

Draft — Not for Implementation

TABLE OF CONTENTS

I.	INTRODUCTION.....	2
II.	BACKGROUND	3
III.	GENERAL PRINCIPLES	4
IV.	OVERALL APPROACH TO MEETING PART 11 REQUIREMENTS	5
V.	STANDARD OPERATING PROCEDURES.....	5
VI.	DATA ENTRY	5
	A. Computer Access Controls.....	5
	B. Audit Trails or other Security Measures	6
	C. Date/Time Stamps.....	7
VII.	SYSTEM FEATURES.....	8
	A. Systems Used for Direct Entry of Data	8
	B. Retrieval of Data and Record Retention.....	8
VIII.	SYSTEM SECURITY	8
IX.	SYSTEM DEPENDABILITY.....	9
	A. Legacy Systems	10
	B. Off-the-Shelf Software.....	10
	C. Change Control.....	11
X.	SYSTEM CONTROLS.....	12
XI.	TRAINING OF PERSONNEL	12
XII.	COPIES OF RECORDS AND RECORD INSPECTION.....	13
XIII.	CERTIFICATION OF ELECTRONIC SIGNATURES	13
	DEFINITIONS	15
	REFERENCES.....	17

Contains Nonbinding Recommendations

Draft — Not for Implementation

**Guidance for Industry¹
Computerized Systems Used in Clinical Trials**

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

I. INTRODUCTION

This document provides guidance about computerized systems that are used to create, modify, maintain, archive, retrieve, or transmit clinical data required to be maintained and/or submitted to the Food and Drug Administration (FDA). These data form the basis for the Agency's decisions regarding the safety and effectiveness of new human and animal drugs, biological products, medical devices, and certain food and color additives. Because the data have broad public health significance, they are expected to be of the highest quality and integrity. This guidance document addresses long-standing FDA regulations concerning clinical trial records. It also addresses requirements of the Electronic Records/Electronic Signatures rule (21 CFR part 11).²

Once finalized, this document will supersede the guidance of the same name issued in April 1999. Revisions will make it consistent with Agency policy as reflected in the guidance for industry on *Part 11, Electronic Records; Electronic Signatures — Scope and Application*, which issued in August 2003, and the Agency's international harmonization efforts.³

¹ This guidance has been prepared by an Agency working group representing the Bioresearch Monitoring Program Managers for each Center within the Food and Drug Administration, the Office of Regulatory Affairs, and the Office of the Commissioner.

² Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations. Part 11 also applies to electronic records submitted to the Agency under the requirements of Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in Agency regulations.

³ In August 2003, FDA issued the guidance for industry entitled *Part 11, Electronic Records; Electronic Signatures—Scope and Application* clarifying that the Agency intended to interpret the scope of part 11 narrowly and to exercise enforcement discretion with regard to part 11 requirements for validation, audit trails, record retention, and record copying. In 1996, the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) issued *E6 Good Clinical Practice: Consolidated Guidance*.

Contains Nonbinding Recommendations

Draft — Not for Implementation

32 FDA's guidance documents, including this guidance, do not establish legally enforceable
33 responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should
34 be viewed only as recommendations, unless specific regulatory or statutory requirements are
35 cited. The use of the word *should* in Agency guidances means that something is suggested or
36 recommended, but not required.

37
38

39 II. BACKGROUND

40

41 FDA has the authority to inspect all records relating to clinical investigations conducted under 21
42 CFR 312, 511.1(b), and 812, regardless of how they were created or maintained (e.g., §§ 312.58,
43 312.68, and 812.145). FDA established the Bioresearch Monitoring (BIMO) Program of
44 inspections and audits to monitor the conduct and reporting of clinical trials to ensure that
45 supporting data from these trials meet the highest standards of quality and integrity, and conform
46 to FDA's regulations. FDA's acceptance of data from clinical trials for decision-making
47 purposes depends on FDA's ability to verify the quality and integrity of the data during FDA on-
48 site inspections and audits. To be acceptable, the data should meet certain fundamental elements
49 of quality whether collected or recorded electronically or on paper. For example, data should be
50 attributable, legible, contemporaneous, original⁴ and accurate.

51

52 This guidance addresses how Agency expectations and regulatory requirements regarding data
53 quality might be satisfied where computerized systems are being used to create, modify,
54 maintain, archive, retrieve, or transmit clinical data. Although the primary focus of this guidance
55 is on computerized systems used at clinical sites to collect data, the principles set forth may also
56 be appropriate for computerized systems belonging to contract research organizations, data
57 management centers, and sponsors. Persons using the data from computerized systems should
58 have confidence that the data are no less reliable than data in paper form.

59

60 Computerized medical devices, diagnostic laboratory instruments, and instruments in analytical
61 laboratories that are used in clinical trials are not the subject of this guidance. This guidance
62 does not address electronic submissions or methods of their transmission to the Agency, except
63 to the degree to which these records comply with Part 11.

64

65 The principles in this guidance may be applied where supporting data or source documents⁵ are
66 created (1) in hardcopy and later entered into a computerized system, (2) by direct entry by a
67 human into a computerized system, and (3) automatically by a computerized system.

68

69

⁴ FDA is allowing original documents to be replaced by certified copies provided the copies are identical and have been verified as such. (see FDA Compliance Policy Guide # 7130.13). See "Definitions" section for a definition of original data.

⁵ Under 21 CFR 312.62 (b) reference is made to records that are part of case histories as "supporting data;" the ICH *E6 Good Clinical Practice* consolidated guidance uses the term "source documents." These terms describe the same information and have been used interchangeably in this guidance.

Contains Nonbinding Recommendations

Draft — Not for Implementation

70 III. GENERAL PRINCIPLES

71
72 The Agency recommends the following general principles with regard to computerized systems
73 that are used to create, modify, maintain, archive, retrieve, or transmit clinical data required to be
74 maintained and/or submitted to FDA.

- 75
- 76 1. We recommend that each study protocol identify at which steps a computerized system
77 will be used to create, modify, maintain, archive, retrieve, or transmit data.
 - 78 2. For each study, we recommend that documentation identify what software and hardware
79 are to be used in computerized systems that create, modify, maintain, archive, retrieve, or
80 transmit data. We also recommend that this documentation be retained as part of the
81 study records.
 - 82 3. We recommend that computerized systems be designed (1) so that all requirements
83 assigned to these systems in a study protocol are satisfied (e.g., data are recorded in
84 metric units, the study blinded) and (2) to preclude errors in data creation, modification,
85 maintenance, archiving, retrieval, or transmission.
 - 86 4. It is important to design a computerized system in such a manner so that all applicable
87 regulatory requirements for record keeping and record retention in clinical trials are met
88 with the same degree of confidence as is provided with paper systems.
 - 89 5. Under 21 CFR 312.62 , 511.1(b)(7)(ii) and 812.140, the clinical investigator must retain
90 records required to be maintained under part 312, § 511.1(b) and § 812, respectively, for
91 a period of time specified in these regulations. Retaining the original source document or
92 a certified copy of the source document at the site where the investigation was conducted
93 can assist in meeting these regulatory requirements. It can also assist in the
94 reconstruction and evaluation of the trial throughout and after the completion of the trial.
 - 95 6. When original observations are entered directly into a computerized system, the
96 electronic record is the source document.
 - 97 7. Records relating to an investigation must be adequate and accurate in the case of
98 investigational new drug applications (INDs) (see § 312.57 and § 312.62), complete in
99 the case of new animal drugs for investigational use (INADs) (see §511.1(b)(7)(ii)), and
100 accurate, complete and current in the case of investigational device exemptions (IDEs)
101 (see § 812.140(a) and § 812.140(b)). An audit trail that is electronic or consists of other
102 physical, logical, or procedural security measures to ensure that only authorized
103 additions, deletions, or alterations of information in the electronic record have occurred
104 may be needed to facilitate compliance with applicable records regulations. Firms should
105 determine and document the need for audit trails based on a risk assessment that takes
106 into consideration circumstances surrounding system use, the likelihood that information
107 might be compromised, and any system vulnerabilities. We recommend that audit trails
108 or other security methods used to capture electronic record activities document who made
109 the changes, when, and why changes were made to the electronic record.
 - 110 8. We recommend that data be retrievable in such a fashion that all information regarding
111 each individual subject in a study is attributable to that subject.

Contains Nonbinding Recommendations

Draft — Not for Implementation

112 9. To ensure the authenticity and integrity of electronic records, it is important that security
113 measures be in place to prevent unauthorized access to the data in the electronic record
114 and to the computerized system.

115

116 **IV. OVERALL APPROACH TO MEETING PART 11 REQUIREMENTS**

117

118 As described in the FDA guidance entitled *Part 11, Electronic Records; Electronic Signatures-*
119 *Scope and Application* (August 2003), while the re-examination of part 11 is underway, FDA
120 intends to exercise enforcement discretion with respect to part 11 requirements for validation,
121 audit trail, record retention, and record copying. That is, FDA does not intend to take
122 enforcement action to enforce compliance with these requirements of part 11 while the agency
123 re-examines part 11. Note that part 11 remains in effect and that the exercise of enforcement
124 discretion applies only to the extent identified in the FDA guidance on part 11. Also, records
125 must still be maintained or submitted in accordance with the underlying requirements set forth in
126 the Federal Food, Drug, and Cosmetic Act (Act), the Public Health Service Act (PHS Act), and
127 FDA regulations (other than part 11), which are referred to in this guidance document as
128 *predicate rules*, and FDA can take regulatory action for noncompliance with such predicate
129 rules.⁶

130

131 Specific details about the Agency’s approach to enforcing part 11 can be found in the *Part 11*
132 *Scope and Application* guidance.

133

134

135 **V. STANDARD OPERATING PROCEDURES**

136

137 We recommend that standard operating procedures (SOPs) pertinent to the use of the
138 computerized system be available on site. We recommend that SOPs be established for the
139 following:

- 140 • System Setup/Installation
- 141 • Data Collection and Handling
- 142 • System Maintenance
- 143 • Data Backup, Recovery, and Contingency Plans
- 144 • Security
- 145 • Change Control
- 146 • Alternative Recording Methods (in the case of system unavailability)

147

148

149 **VI. DATA ENTRY**

150

151 **A. Computer Access Controls**

152

⁶ This term refers to underlying requirements set forth in the Federal Food, Drug, and Cosmetic Act, the PHS Act, and FDA regulations (other than 21 CFR Part 11). Regulations governing good clinical practice and human subject protection can be found at 21 CFR parts 50, 56, 312, 511, and 812. See Definitions section at the end of this document listing definitions of this and other terms used in this guidance.

Contains Nonbinding Recommendations

Draft — Not for Implementation

153 To ensure that individuals have the authority to proceed with data entry, data entry systems must
154 be designed to limit access so that only authorized individuals are able to input data
155 (§ 11.10(d)).⁷ Examples of methods for controlling access include using combined identification
156 codes/passwords or biometric-based identification at the start of a data entry session. Controls
157 and procedures must be in place that are designed to ensure the authenticity and integrity of
158 electronic records created, modified, maintained, or transmitted using the data entry system
159 (§ 11.10). Therefore, we recommend that each user of the system have an individual account
160 into which the user logs-in at the beginning of a data entry session, inputs information (including
161 changes) on the electronic record, and logs out at the completion of data entry session.
162

163 We recommend that individuals work only under their own password or other access key and not
164 share these with others. We recommend that individuals not be allowed to log onto the system to
165 provide another person access to the system. We also recommend that passwords or other access
166 keys be changed at established intervals.
167

168 When someone leaves a workstation, we recommend that the SOP require that person to log off
169 the system. Alternatively, an automatic log off may be appropriate for long idle periods. For
170 short periods of inactivity, we recommend that some kind of automatic protection be installed
171 against unauthorized data entry. An example could be an automatic screen saver that prevents
172 data entry until a password is entered.
173

B. Audit Trails or other Security Measures

174
175
176 Section 11.10(e) requires persons who use electronic record systems to maintain an audit trail as
177 one of the procedures to protect the authenticity, integrity, and, when appropriate, the
178 confidentiality of electronic records. As clarified in the *Part 11 Scope and Application* guidance,
179 however, the Agency intends to exercise enforcement discretion regarding specific part 11
180 requirements related to computer-generated, time-stamped audit trails (§ 11.10(e), (k)(2) and any
181 corresponding requirement in § 11.30). Persons must still comply with all applicable predicate
182 rule requirements for clinical trials, including, for example, that records related to the conduct of
183 the study must be adequate and accurate (§§ 312.57, 312.62, and 812.140). It is therefore
184 important to keep track of all changes made to information in the electronic records that
185 document activities related to the conduct of the trial. Computer-generated, time-stamped audit
186 trails or information related to the creation, modification, or deletion of electronic records may
187 be useful to ensure compliance with the appropriate predicate rule.
188

189 In addition, clinical investigators must, upon request by FDA, at reasonable times, permit agency
190 employees to have access to, and copy and verify any required records or reports made by the
191 investigator (§§ 312.68, 511.1(b)(7)(ii) and 812.145). In order for the Agency to review and
192 copy this information, FDA personnel should be able to review audit trails or other documents
193 that track electronic record activities both at the study site and at any other location where
194 associated electronic study records are maintained. To enable FDA's review, information about
195 the creation, modification, or deletion of electronic records should be created incrementally, and
196 in chronological order. To facilitate FDA's inspection of this information, we recommend that

⁷ As FDA announced in the *Part 11 Scope and Application* guidance, we intend to enforce certain controls for closed systems in § 11.10, including § 11.10(d).

Contains Nonbinding Recommendations

Draft — Not for Implementation

197 clinical investigators retain either the original or a certified copy of any documentation created to
198 track electronic records activities.

199
200 Even if there are no applicable predicate rule requirements, it may be important to have
201 computer-generated, time-stamped audit trails or other physical, logical, or procedural security
202 measures to ensure the trustworthiness and reliability of electronic records. We recommend that
203 any decision on whether to apply computer-generated audit trails or other appropriate security
204 measures be based on the need to comply with predicate rule requirements, a justified and
205 documented risk assessment, and a determination of the potential effect on data quality and
206 record integrity. Firms should determine and document the need for audit trails based on a risk
207 assessment that takes into consideration circumstances surrounding system use, the likelihood
208 that information might be compromised, and any system vulnerabilities.

209
210 If you determine that audit trails or other appropriate security measures are needed to ensure
211 electronic record integrity, we recommend that personnel who create, modify, or delete
212 electronic records not be able to modify the documents or security measures used to track
213 electronic record changes. We recommend that audit trails or other security methods used to
214 capture electronic record activities document who made the changes, when, and why changes
215 were made to the electronic record.

216
217 Some examples of methods for tracking changes to electronic records include:

- 218
219
- Computer-generated, time-stamped electronic audit trails.
 - Signed and dated printed versions of electronic records that identify what, when, and by whom changes were made to the electronic record. When using this method, it is important that appropriate controls be utilized that ensure the accuracy of these records (e.g., sight verification that the printed version accurately captures all of the changes made to the electronic record).
 - Signed and dated printed standard electronic file formatted versions (e.g., pdf, xml or sgml) of electronic records that identify what, when, and by whom changes were made to the electronic record.
 - Procedural controls that preclude unauthorized personnel from creating, modifying, or deleting electronic records or the data contained therein.
- 220
221
222
223
224
225
226
227
228
229

C. Date/Time Stamps

230
231
232
233 We recommend that controls be put in place to ensure that the system's date and time are correct.
234 The ability to change the date or time should be limited to authorized personnel and such
235 personnel should be notified if a system date or time discrepancy is detected. We recommend
236 that someone always document changes to date or time. We do not expect documentation of
237 time changes that systems make automatically to adjust to daylight savings time conventions.

238 We also recommend that dates and times include the year, month, day, hour, and minute. The
239 Agency encourages establishments to synchronize systems to the date and time provided by
240 trusted third parties.

Contains Nonbinding Recommendations

Draft — Not for Implementation

241 Clinical study computerized systems are likely be used in multi-center trials and may be located
242 in different time zones. For systems that span different time zones, it is better to implement time
243 stamps with a clear understanding of the time zone reference used. We recommend that system
244 documentation explain time zone references as well as zone acronyms or other naming
245 conventions.
246

247 248 **VII. SYSTEM FEATURES**

249
250 The Agency recommends that a number of computerized system features be available to
251 facilitate the collection, inspection, review, and retrieval of quality clinical data. Key features
252 are described here.
253

254 **A. Systems Used for Direct Entry of Data**

255
256 We recommend that prompts, flags, or other help features be incorporated into the computerized
257 system to encourage consistent use of clinical terminology and to alert the user to data that are
258 out of acceptable range. We recommend against the use of features that automatically enter data
259 into a field when the field is bypassed.
260

261 **B. Retrieval of Data and Record Retention**

262
263 FDA expects to be able to reconstruct a clinical study submitted to the agency. This means that
264 documentation, such as that described in the General Principles, Sections III.1, III.2 and III.5,
265 should fully describe and explain how data were obtained and managed and how electronic
266 records were used to capture data. We suggest that your decision on how to maintain records be
267 based on predicate rule requirements and that this documented decision be based on a justified
268 risk assessment and a determination of the value of the records over time. As explained in the
269 Part 11 Scope and Application guidance, FDA does not intend to object to required records that
270 are archived in electronic format; nonelectronic media such as microfilm, microfiche, and paper;
271 or to a standard electronic file format (such as PDF, XML, or SGML). Persons must still comply
272 with all predicate rule requirements, and the records themselves and any copies of required
273 records should preserve their original content and meaning. Paper and electronic record and
274 signature components can co-exist (i.e., as a hybrid system) as long as the predicate requirements
275 (21 CFR parts 50, 56, 312, 511, and 812) are met, and the content and meaning of those records
276 are preserved.
277

278 It is not necessary to reprocess data from a study that can be fully reconstructed from available
279 documentation. Therefore, actual application software, operation systems, and software
280 development tools involved in processing of data or records do not need to be retained.
281

282 283 **VIII. SYSTEM SECURITY**

284
285 In addition to internal safeguards built into the computerized system, external safeguards should
286 be put in place to ensure that access to the computerized system and to the data is restricted to

Contains Nonbinding Recommendations

Draft — Not for Implementation

287 authorized personnel as required by 21 CFR 11.10(d). We recommend that staff be kept
288 thoroughly aware of system security measures and the importance of limiting access to
289 authorized personnel.

290
291 SOPs should be developed and implemented for handling and storing the system to prevent
292 unauthorized access. Controlling system access can be accomplished through the following
293 provisions of part 11 that, as discussed in the part 11 guidance, FDA intends to continue to
294 enforce:

- 295 • Operational system checks (§ 11.10(f));
- 296 • Authority checks (§ 11.10(g));
- 297 • Device (e.g., terminal) checks (§ 11.10(h)); and
- 298 • The establishment of and adherence to written policies that hold individuals
299 accountable for actions initiated under their electronic signatures (§ 11.10(j)).

300
301 The Agency recommends that access to data be restricted and monitored through the system's
302 software with its required log-on, security procedures, and audit trail (or other selected security
303 measures to track electronic record activities). We recommend that procedures and controls be
304 implemented to prevent the data from being altered, browsed, queried, or reported via external
305 software applications that do not enter through the protective system software.

306
307 We recommend that a cumulative record be available that indicates, for any point in time, the
308 names of authorized personnel, their titles, and a description of their access privileges. We
309 recommend that the record be kept in the study documentation, accessible at the site.

310
311 If a sponsor supplies computerized systems exclusively for clinical trials, we recommend that the
312 systems remain dedicated to the purpose for which they were intended and validated. If a
313 computerized system being used for a clinical study is part of a system normally used for other
314 purposes, we recommend that efforts be made to ensure that the study software be logically and
315 physically isolated as necessary to preclude unintended interaction with nonstudy software. If
316 any of the software programs are changed, we recommend that the system be evaluated to
317 determine the effect of the changes on logical security.

318
319 We recommend that controls be implemented to prevent, detect, and mitigate effects of computer
320 viruses, worms, or other potentially harmful software code on study data and software.

321

322

IX. SYSTEM DEPENDABILITY

324

325 The Agency recommends that sponsors ensure and document that all computerized systems
326 conform to their own established requirements for completeness, accuracy, reliability, and
327 consistent intended performance.

328

329 We recommend that systems documentation be readily available at the site where clinical trials
330 are conducted and provide an overall description of the computerized systems and the
331 relationships among hardware, software, and physical environment.

332

Contains Nonbinding Recommendations

Draft — Not for Implementation

333 As noted in the *Part 11 Scope and Application* guidance, the Agency intends to exercise
334 enforcement discretion regarding specific part 11 requirements for validation of computerized
335 systems. We suggest that your decision to validate computerized systems and the extent of the
336 validation take into account the impact the systems have on your ability to meet predicate rule
337 requirements. You should also consider the impact those systems might have on the accuracy,
338 reliability, integrity, availability, and authenticity of required records and signatures. Even if
339 there is no predicate rule requirement to validate a system, it may still be important to validate
340 the system, based on criticality and risk, to ensure the accuracy, reliability, integrity, availability
341 and authenticity of required records and signatures.

342
343 We recommend that you base your approach on a justified and documented risk assessment and
344 determination of the potential of the system to affect data quality and record integrity. For
345 example, in the case where data are directly entered into electronic records and the business
346 practice is to rely on the electronic record, validation of the computerized system is important.
347 However when a word processor is used to generate SOPs for use at the clinical site, validation
348 would not be important.

349
350 If validation is required, FDA may ask to see the regulated company's documentation that
351 demonstrates software validation. The study sponsor is responsible for making any such
352 documentation available if requested at the time of inspection at the site where software is used.
353 Clinical investigators are not generally responsible for validation unless they originated or
354 modified software.

A. Legacy Systems

355
356
357
358 As noted in the *Part 11 Scope and Application* guidance, the Agency intends to exercise
359 enforcement discretion with respect to all part 11 requirements for systems that otherwise were
360 fully operational prior to August 20, 1997, the effective date of part 11, under the circumstances
361 described below. These systems are also known as legacy systems. The Agency does not intend
362 to take enforcement action to enforce compliance with any part 11 requirements if all the
363 following criteria are met for a specific system:

- 364
365
- 366 • The system was in operation before the part 11 effective date.
 - 367 • The system met all applicable predicate rule requirements prior to the part 11 effective date.
 - 368 • The system currently meets all applicable predicate rule requirements.
 - 369 • There is documented evidence and justification that the system is fit for its intended use.

370 If a system has changed since August 20, 1997, and if the changes would prevent the system
371 from meeting predicate rule requirements, part 11 controls should be applied to part 11 records
372 and signatures pursuant to the enforcement policy expressed in the part 11 guidance. Please refer
373 to the *Part 11 Scope and Application* guidance for further information.

B. Off-the-Shelf Software

374
375
376
377 While the Agency has announced that it intends to exercise enforcement discretion regarding
378 specific part 11 requirements for validation of computerized systems, persons must still comply

Contains Nonbinding Recommendations

Draft — Not for Implementation

379 with all predicate rule requirements for validation. We suggested in the guidance for industry on
380 part 11 that the impact of computerized systems on the accuracy, reliability, integrity,
381 availability, and authenticity of required records and signatures be considered when you decide
382 whether to validate, and noted that even absent a predicate rule requirement to validate a system,
383 it might still be important to validate in some instances.

384
385 For most off-the-shelf software, the design level validation will have already been done by the
386 company that wrote the software. Given the importance of ensuring valid clinical trial data,
387 FDA suggests that the sponsor or contract research organization (CRO) have documentation
388 (either original validation documents or on-site vendor audit documents) of this design level
389 validation by the vendor and would itself have performed functional testing (e.g., by use of test
390 data sets) and researched known software limitations, problems, and defect corrections. Detailed
391 documentation of any additional validation efforts performed by the sponsor or CRO will
392 preserve the findings of these efforts.

393
394 In the special case of database and spreadsheet software that is: (1) purchased off-the-shelf, (2)
395 designed for and widely used for general purposes, (3) unmodified, and (4) not being used for
396 direct entry of data, the sponsor or contract research organization may not have documentation of
397 design level validation. FDA suggests that the sponsor or contract research organization perform
398 functional testing (e.g., by use of test data sets) and research known software limitations,
399 problems, and defect corrections.

400
401 In the case of off-the-shelf software, we recommend that the following be available to the
402 Agency on request:

- 403
- 404 • A written design specification that describes what the software is intended to do and how
405 it is intended to do it;
 - 406 • A written test plan based on the design specification, including both structural and
407 functional analysis; and
 - 408 • Test results and an evaluation of how these results demonstrate that the predetermined
409 design specification has been met.

410 Additional guidance on general software validation principles can be found in FDA's guidance
411 entitled *General Principles of Software Validation; Final Guidance for Industry and FDA Staff*.

412

C. Change Control

414

415 FDA recommends that written procedures be put in place to ensure that changes to the
416 computerized system, such as software upgrades, including security and performance patches,
417 equipment, or component replacement, or new instrumentation, will maintain the integrity of the
418 data and the integrity of protocols. We recommend that the effects of any changes to the system
419 be evaluated and a decision made regarding whether, and if so, what level of validation activities
420 related to those changes would be appropriate. We recommend that validation be performed for
421 those types of changes that exceed previously established operational limits or design
422 specifications. Finally, we recommend that all changes to the system be documented.

423

Contains Nonbinding Recommendations

Draft — Not for Implementation

424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469

X. SYSTEM CONTROLS

The Agency recommends that appropriate system control measures be developed and implemented.

- Software Version Control

We recommend that measures be put in place to ensure that versions of software used to generate, collect, maintain, and transmit data are the versions that are stated in the systems documentation.

- Contingency Plans

We recommend that written procedures describe contingency plans for continuing the study by alternate means in the event of failure of the computerized system.

- Backup and Recovery of Electronic Records

When electronic formats are the only ones used to create and preserve electronic records, the Agency recommends that backup and recovery procedures be outlined clearly in SOPs and be sufficient to protect against data loss. We also recommend that records be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data. We recommend that records be stored at a secure location specified in the SOPs. Storage is typically offsite or in a building separate from the original records.

We recommend that backup and recovery logs be maintained to facilitate an assessment of the nature and scope of data loss resulting from a system failure.

Firms that rely on electronic and paper systems should determine the extent to which backup and recovery procedures are needed based on the need to meet predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on data quality and record integrity.

XI. TRAINING OF PERSONNEL

Under 21 CFR 11.10(i), firms using computerized systems must determine that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks.

The Agency recommends that training be provided to individuals in the specific operations with regard to computerized systems that they are to perform. We recommend that training be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerized system and with any changes to the system during the course of the study.

Contains Nonbinding Recommendations

Draft — Not for Implementation

470 We recommend that employee education, training, and experience be documented.

471

472

XII. COPIES OF RECORDS AND RECORD INSPECTION

473

474
475 FDA has the authority to inspect all records relating to clinical investigations conducted under 21
476 CFR Parts 312 and 812, regardless of how the records were created or maintained (21 CFR
477 312.58, 312.68, and 812.145). Therefore, you should provide the FDA investigator with
478 reasonable and useful access to records during an FDA inspection. As noted in the *Part 11,*
479 *Electronic Records; Electronic Signatures- Scope and Application* guidance, the Agency intends
480 to exercise enforcement discretion with regard to specific part 11 requirements for generating
481 copies of records (§ 11.10(b) and any corresponding requirement in § 11.30). We recommend
482 that you supply copies of electronic records by:

483

484 • Producing copies of records held in common portable formats when records are
485 maintained in these formats

486 • Using established automated conversion or export methods, where available, to make
487 copies available in a more common format (e.g., pdf, xml, or sgml formats)

488

489 Regardless of the method used to produce copies of electronic records, it is important that the
490 copying process used produces copies that preserve the content and meaning of the record. For
491 example, if you have the ability to search, sort, or trend records, copies given to FDA should
492 provide the same capability if it is reasonable and technically feasible. FDA expects to inspect,
493 review, and copy records in a human readable form at your site, using your hardware and
494 following your established procedures and techniques for accessing records.

495

496 We recommend you contact the Agency if there is any doubt about what file formats and media
497 the Agency can read and copy.

498

499

XIII. CERTIFICATION OF ELECTRONIC SIGNATURES

500

501
502 As required by 21 CFR 11.100(c), persons using electronic signatures to meet an FDA signature
503 requirement must, prior to or at the time of such use, certify to the Agency that the electronic
504 signatures in their system, used on or after August 20, 1997, are intended to be the legally
505 binding equivalent of traditional handwritten signatures.

506

507 As set forth in § 11.100(c)(1), the certification must be submitted in paper, signed with a
508 traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers
509 Lane, Rockville, Maryland 20857. The certification is to be submitted prior to or at the time
510 electronic signatures are used. However, a single certification can be used to cover all electronic
511 signatures used by persons in a given organization. This certification is created by persons to
512 acknowledge that their electronic signatures have the same legal significance as their traditional
513 handwritten signatures. See the following example of a certification statement:

514

Contains Nonbinding Recommendations

Draft — Not for Implementation

515 Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations,
516 this is to certify that [name of organization] intends that all electronic
517 signatures executed by our employees, agents, or representatives, located
518 anywhere in the world, are the legally binding equivalent of traditional
519 handwritten signatures.

520

521

522

523

524

525

Contains Nonbinding Recommendations

Draft — Not for Implementation

526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571

DEFINITIONS

The following is a list of definitions for terms as they are used in, and for the purposes of, this guidance document.

Attributable Data: Attributable data are those that can be traced to individuals responsible for observing and recording the data. In an automated system, attributability could be achieved by a computer system designed to identify individuals responsible for any input.

Audit Trail: An *audit trail* is a secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record.

Certified Copy: A copy of original information that has been verified, as indicated by dated signature, as an exact copy having all of the same attributes and information as the original

Computerized System: A *computerized system* includes computer hardware, software, and associated documents (e.g., user manual) that create, modify, maintain, archive, retrieve, or transmit in digital form information related to the conduct of a clinical trial.

Direct Entry: Recording data where an electronic record is the original capture of the data. Examples are the keying by an individual of original observations into the system, or automatic recording by the system of the output of a balance that measures subject's body weight.

Electronic Record: 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.

Electronic Signature: 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.

Original data: *Original data* are those values that represent the first recording of study data. FDA is allowing original documents and the original data recorded on those documents to be replaced by certified copies provided the copies are identical and have been verified as such. (see FDA Compliance Policy Guide # 7130.13

Predicate rule: This term refers to underlying requirements set forth in the Federal Food, Drug, and Cosmetic Act, the PHS Act, and FDA regulations (other than 21 CFR part 11). Regulations governing good clinical practice and human subject protection can be found at 21 CFR parts 50, 56, 312, 511, and 812.

Software Validation: Confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses and that the particular

Contains Nonbinding Recommendations

Draft — Not for Implementation

572 requirements implemented through the software can be consistently fulfilled. *Design level*
573 *validation* is that portion of the software validation that takes place in parts of the software life
574 cycle before the software is delivered to the end user.

575
576 **Source Documents:** Original documents and records including, but not limited to, hospital
577 records, clinical and office charts, laboratory notes, memoranda, subjects' diaries or evaluation
578 checklists, pharmacy dispensing records, recorded data from automated instruments, copies or
579 transcriptions certified after verification as being accurate and complete, microfiches,
580 photographic negatives, microfilm or magnetic media, x-rays, subject files, and records kept at
581 the pharmacy, at the laboratories, and at medico-technical departments involved in the clinical
582 trial.

583
584 **Transmit:** *Transmit* is to transfer data within or among clinical study sites, contract research
585 organizations, data management centers, or sponsors. Other Agency guidance covers
586 transmission from sponsors to the Agency.

587

Contains Nonbinding Recommendations

Draft — Not for Implementation

588
589
590
591

592
593

594
595

596
597

598

599

600

601

602

603
604

605

606

607

REFERENCES

FDA, *21 CFR Part 11, "Electronic Records; Electronic Signatures; Final Rule."* *Federal Register* Vol. 62, No. 54, 13429, March 20, 1997.

FDA, *Compliance Program Guidance Manual, "Compliance Program 7348.810 - Sponsors, Contract Research Organizations and Monitors,"* October 30, 1998.

FDA, *Compliance Program Guidance Manual, "Compliance Program 7348.811 - Bioresearch Monitoring - Clinical Investigators,"* September 2, 1998.

FDA, *Glossary of Computerized System and Software Development Terminology,* 1995.

FDA, *Good Clinical Practice VICH GL9,* 2001.

FDA, *Guideline for the Monitoring of Clinical Investigations,* 1988.

FDA, *Information Sheets for Institutional Review Boards and Clinical Investigators,* 1998.

FDA, *Software Development Activities,* 1987.

International Conference on Harmonisation, "E6 Good Clinical Practice: Consolidated Guideline," *Federal Register,* Vol. 62, No. 90, 25711, May 9, 1997.

FDA, *Part 11, Electronic Records; Electronic Signatures — Scope and Application,* 2003.

FDA, *General Principles of Software Validation; Guidance for Industry and FDA Staff,* 2002.