



GENZYME CORPORATION
ONE KENDALL SQUARE
CAMBRIDGE, MA 02139-1562, U.S.A.
617-252-7500
FAX 617-252-7600

Dockets Management Branch
HFA-305
Food and Drug Administration
5630 Fishers Lane
Room 1061
Rockville, MD 20852

Subject: Docket No. 2004N-0133
“Electronic Record; Electronic Signatures; Public Meeting”

11 May 2004

Dear Sir/Madam:

Genzyme respectfully submits comments to and suggestions for modifications to 21 CFR Part 11. There have been many challenges in interpreting and implementing these regulatory requirements. However, if taken in the spirit of which the regulation was originally written, we believe there is value in retaining the regulation as some aspects continue to make sound computer system management sense. Below please see our comments regarding the questions posed in the April 8, 2004 Federal Register Notice, as well as a line-by-line analysis of recommended changes to the regulation itself. Genzyme appreciates this opportunity to comment.

1. *Subpart A 1.* We agree with FDA’s classification of records based on use. We note that it is common to use electronic records in combination with paper records – electronic distribution of SOPs where the signatures are handwritten on paper, or electronic filings, where the signoffs are handwritten on paper, for example. In this scenario, the system containing the electronic originals and distributing the electronic renditions would be considered “in use” to meet FDA requirements. Users have only an electronic copy to relate to, may use that electronic version from an on-line source and a printed version is good only until the next electronic revision. Genzyme has consistently emphasized that predicate rule requirements should be considered as the foundation for whether Part 11 controls apply to any system, including those listed above. We believe that Part 11 should emphasize that controls application is both predicate rule and use driven, and that use is considered in the context of patient safety and product quality.
2. *Subpart A 2.* Please see Line by Line Comments below.
3. *Subpart A 3.*
 - a. Validation – All computer system management practices should be driven by the desire to assure data integrity and system reliability. Computer system testing of some sort (whether rising to the level of “formal validation” or some other procedurally prescribed commissioning) should be performed, regardless of perceived predicate rule requirements. A sound risk assessment and management process should prescribe the degree to which this commissioning is performed. Genzyme suggests that Part 11 be revised to indicate that computer systems providing FDA-reviewable information should be qualified/validated/tested to the degree dictated by sound risk management practice, taking into account the need to assure data

2004N-0133

Docket No. 2004N-0133
“Electronic Record; Electronic Signatures; Public Meeting”
Page 1 of 9

C2

integrity, system reliability and patient safety/product quality.

- b. Audit Trails – We believe that the use of audit trails should be based on considerations of what value they will provide for the users and maintainers of the system. Hybrid audit trail approaches (paper change control on an electronic environment) can provide the same degree of traceability and accountability as that of an automatically generated audit trail. For example, in complex MRP environments, it may make more business sense to use audit trails, properly tested, as a replacement to paper change control, simply due to transaction volume. Genzyme recognizes that predicate rules require traceability in a number of areas and if an organization chooses to use an electronic system to replace a paper process and traceability is required, an electronic audit trail is required. However, we believe that organizations should reach that conclusion, based on regulatory compliance and business value.
 - c. Record Retention – We are in agreement with the current guidance and reiterate that record retention media can take any stable physical form. Reduction of the electronic records to non-electronic media needs to allow individuals who engage in future reviews to come to the same conclusion as individuals who used the information real-time, in its native environment.
 - d. Record Copies – We are in agreement with the guidance that record copies to the Agency can take any physical form so long as that physical form would contain adequate information and metadata for the Agency to be able to review the content in the appropriate context, and draw the same conclusions. It would be helpful for the Agency to acknowledge sole responsibility for the integrity of records once electronic copies have been received by the Agency, as the Organization that supplied the records no longer controls them.
 - e. Records Required by Predicate Rules – In some cases, required records are very explicitly listed in the CFR. Most companies then add record requirements via internal SOPs as part of the interpretation of the less clear requirements. Genzyme respectfully suggests that the Agency consider providing an explicit definition of record scope, for example, stating that predicate rules as codified in the Code of Federal Regulations and *any SOPs written as interpretive of those predicate rules, that also mandate records*, are considered records subject to Part 11, should they be implemented electronically. This would serve to provide a “bright line” for what is in versus out of scope on predicate rules. The degree to which Part 11 controls would be applied, whether the record is prescribed by CFR or SOP, would be governed by a risk management process.
4. *Subpart B 1, 2.* Genzyme Corporation believes that risk management processes should be used across the computer system lifecycle and not limited to specific parts of Part 11. We respectfully suggest that the Agency revise the regulation to allow organizations to consider what features and components of Part 11 should be implemented, based on risk assessment. Accordingly, areas of non-negotiability would be limited to physical requirements for e-identity, e-signature, audit trails, etc., and where needed to assure data integrity and information traceability. Please see additional Line by Line Comments below.
 5. *Subpart B 3.* As previously stated, Genzyme requests that FDA formally recognize that an organization’s chain of custody is broken once FDA takes possession of that organization’s electronic records. We suggest that Part 11 wording be modified to state that electronic records for submission should be prepared and maintained within the company under Part 11 requirements. However, after FDA takes possession of the records, the company ceases to assume further responsibility for data integrity. FDA then has the right to determine what controls, if any, they place on the electronic records for which they have assumed responsibility, in concert with predicate rules, associated guidance

documents and their need to protect the integrity of the electronic records they now possess.

6. *Subpart B 4.* We believe there should be no distinction between open and closed systems. Please see Line by Line Comments below.
 - a. *Subpart B Individual Controls 1.* We note that organizations that are using computer systems to manage information being relied on to make regulatory decisions often decide to validate to allay data integrity and system reliability concerns irrespective of an overt predicate rule requiring validation. We suggest that §11.10(b) could be removed or modified to state that validation should be based on predicate rule requirements and an appropriate risk management process.
 - b. *Subpart B Individual Controls 2.* See comments above on Record Retention and Record Copies as well as Line by Line Comments below.
 - c. *Subpart B Individual Controls 3.* Audit trails are used to meet several needs including traceability of an operator to an action, a history of the transaction's effect on the data point, forensically to determine behavior patterns, and replacing "initials and dates" for the appropriate transactions. Forensic use of an audit trail can provide insight into some of the unauthorized record events listed, however we believe that forcing an audit trail into this role is too specific of a construction. Genzyme recommends the Agency provide language that identifies unacceptable kinds of weaknesses, and leave to the Organization the choice of what technologies/processes it could use to minimize exposure to those weaknesses.
 - d. *Subpart B Individual Controls 4.* Please see Line by Line Comments below.
7. *Subpart C.* Genzyme recommends the Agency provide language that identifies what kinds of security issues would be unacceptable, and leave to the Organization the choice of what technologies/processes it could use to minimize or prevent exposure to those issues.
8. *Additional Questions for Comment*
 - a. Economics of Modifying This Document – Genzyme will evolve its risk management processes to respond to whatever changes occur; therefore economic impact should be minimal.
 - b. Clarification of Part 11 Record Types – Please see Records Required by Predicate Rules above.
 - c. How does Part 11 Discourage Innovation? – We believe that Part 11 can influence or discourage innovation in a variety of ways.
 - i. Initial perceptions that Part 11 is an all or nothing regulation, for example, implementation of requirements in the regulation was not based on concerns for the relative worth/value of the controls to the data and by extension, to the patient and business.
 - ii. Organizations felt that the burden of implementing controls was easier to avoid by not installing new technology that might be subject to it.
 - iii. A belief arose that the cost to make changes to a system to comply to Part 11 outweighed the benefits of making those changes.
 - iv. Paper systems were kept alive despite a redundant electronic system because of fears that the electronic system was "not compliant," thereby wasting resources by duplicating efforts.

- d. What Potential Changes Could Encourage Innovation? – Genzyme Corporation believes that Part 11 should encourage innovation within a state of control that allows companies to exercise discretion based on sound science and technological capabilities. Part 11 should address practical concerns and not prescribe what technology should be used to satisfy those concerns. As such, we would like to have additional guidance specifying those undesirable consequences the Agency does not want to see. By indicating what the undesirable outcomes are, a company is then free to develop methods and technologies for minimizing or removing those unacceptable events.
- e. What risk-based approaches would help to ensure electronic record integrity and electronic signature authenticity? – We note that risk assessment and management is a process and no single method can ensure electronic record integrity and electronic signature authenticity. Although any one of several risk assessment methods can be used to identify weaknesses to mitigate or opportunities to enhance integrity, of greater importance is that the organization understands the fundamentals of risk management and can then logically apply that mindset to preserving data integrity and electronic signature authenticity. Genzyme suggests that revised Part 11 language list risk management characteristics or concepts that would be desirable to have as part of a risk management program and leave the selection of the tool(s) used to meet those characteristics up to the organization.
- f. What are the concerns about legacy systems? – Genzyme believes that pragmatic application of procedural and technical controls makes a discussion of legacy systems a moot point, regardless of system age. Users / data owners that have a large stake in the integrity of the system content should have controls in place that engender a high degree of confidence in the system content and performance. We note that it is becoming increasingly hard to find a true legacy (pre-1997, unchanged) computer system since any business has to engage in some level of configuration and change management to keep the system up and running. Genzyme suggests that use of the phrase “legacy systems” be restricted to guidance as descriptive only of environments that are not Part 11 compliant, regardless of chronological age.
- g. Should Part 11 address record conversion? – Genzyme does not believe that prescriptively addressing record conversion is helpful. Instead, we recommend the Agency suggest that e-record conversion and/or migration is a data manipulation process that, like software upgrades, needs to be managed and controlled to assure the resulting information is accurate. A business decision to convert or migrate should remain with the system owner *as long as content and meaning of the records and signatures is present and not subject to change*, regardless of the outcome, as indicated in the Guidance,. It should be noted that data migration and/or conversion are often done in order for a new system or upgrade to be useful to the business, so that the issue is not about meeting Part 11 requirements, but rather how much the information is needed on a day to day basis.
- h. Are there provisions of Part 11 that should be deleted based on the availability of new technologies? – Please see below.

Rule Line by Line Comment Form

Section	Paragraph Figure/ Table Line No.	Proposed Change	Comment/ Rationale
11.1(b)	lines 9-10	This part applies to electronic records that are created or otherwise managed to meet predicate rule requirements.	All the listed states of a record lifecycle are unnecessary at this point in the document (rely on 11.3(b)(6)).
11.1(b)	11-13	Remove sentence.	Focus scope on predicate rules as interpreted through CFR.
11.1(b)	14-15	Specifically call out paper-initiated FAXes that result in paper output.	Paper to paper is out of scope – paper to electronic may be in scope.
11.1(c)	19	Add “the legally binding” in front of equivalent; remove initials, and other general signings.	Clarification and to minimize confusion surrounding full handwritten signatures as opposed to “initialing and dating,” which is more often a means of identification of an operator than the “signing” of a significant event such as approved, rejected or released.
		Add language to recognize that electronic identity carries a legal connotation, whether by audit trail capture of user ID or input of user ID as a check off.	Electronic identity is often confused with electronic signature as the components used to establish both (password and ID) can sometimes be the same. We believe this suggested language will enable differentiation between the two.
11.2(a)	32-35	Rewrite – Electronic records and electronic signatures may be used for records submitted to the Agency as well as for records required under predicate rules but not submitted. These electronic records and electronic signatures must be implemented and used in such a way as to demonstrate a high degree of assurance in the information and signature integrity.	The goal is data and signature integrity, in the context of electronic records. Emphasizing this point earlier sets the proper framework.

Section	Paragraph Figure/ Table Line No.	Proposed Change	Comment/ Rationale
11.3(b) (4),(9)	70-71, 87-89	Remove.	The concepts of open versus closed systems have little meaning in light of electronic systems that span the globe, traverse leased lines and may rely on “quasi-employees” to do data entry, such as with clinical trial data, patient registries, etc.
11.3(b) (5)	72-74	Remove.	There are established industry definitions for this phrase, and its value is questionable if open and closed definitions are removed.
11.10	92	Remove the word “closed.”	See rationale above.
11.10	94	Remove the word “closed.”	See rationale above.
11.10(a)	100-101	Rewrite or remove – computer systems that contain electronic records for predicate rule use shall be validated to an extent which assures the electronic records (and electronic signatures, as appropriate) are created, maintained and retired in an accurate and integral manner or remove and point to predicate rules.	The goal of validation is to provide documented assurance that a computer system performs the way it is expected to, and that any data created, managed or archived is done so in a way that meets regulatory and business needs. We believe that it is of limited value to restate premise here.
11.10(b)	103-106	Rewrite – electronic or paper copies of electronic records used to meet regulatory requirements should be available to the Agency for inspection, review and copying <i>as long as the copies provide the same context and meaning</i> to the user.	Technology may not permit giving electronic copies to Agency personnel. However, paper printouts of the electronic records should be acceptable as long as Agency personnel are provided the same context (in terms of information) from which to draw a conclusion as the supplying organization had.

Section	Paragraph Figure/ Table Line No.	Proposed Change	Comment/ Rationale
11.10(c)	107-108	Expand – protection of records to enable their accurate and ready retrieval throughout the record retention period by either electronic or hardcopy means.	Technology may limit the ability of an organization to store electronic records electronically for the defined record retention periods specified in different regulations. Printing records to paper is an acceptable method of retaining these records as long as the information printed out provides the same context for interpreting the information as was available at the time of the electronic record’s creation.
11.10(f)	116-117	Remove.	Operational system checks are no longer a relevant distinction to make regarding software performance – good validation practices should dictate the testing required to meet user requirements regarding batch processing.
11.10(g)	118-120	Simplify – use good security technology and practices to assure that only authorized individuals can use a system, electronically sign a record or otherwise effect the content or operation of the computer system.	Current verbiage implies these are all stand-alone, discrete items or activities. We believe that good security management covers all these scenarios.
11.10(h)	121-122	Remove entirely or replace with a statement indicating that connected devices shall be managed through a program that provides documented assurance that field equipment is correctly configured and provides accurate data to the computer system.	Device or terminal checking is effectively covered through other areas of the GMPs, e.g., through Metrology programs.
11.10(j)	126-128	Remove “in order to deter record and signature falsification.”	Written documents don’t deter falsification in and of themselves – they provide notice unacceptable activity and potential consequences.
11.10(k)	129-133	Condense to require something like “adequate revision and use controls for internal and external system documentation.”	Broadly covers both internal SOP and procedure systems as well as vendor manuals/CDs/online use information.
11.30	136-145	Remove section.	See definitions above.

Section	Paragraph Figure/ Table Line No.	Proposed Change	Comment/ Rationale
11.70	164	Substitute the word “linked” with “traceable” as electronic signatures should be electronically associated with or affixed to the electronic records they support.	The word link has often caused confusion and with hybrid systems, signatures on paper are associated with the electronic records that created the printouts. Hence traceability is the larger issue.
Subpart C	General Comment	Distinguish between the general requirements for electronic signatures versus the general requirements for electronic identity (i.e., login credentials). Similarly, in describing characteristics, break technology down into two or more component combinations versus single component identifications/e-signatures.	Not every transaction that requires a user ID and password or captures electronic identity is a signing event. Required signatures are spelled out via predicate rules, in house procedures, and are attested to events, as opposed to establishing electronic identity that may then be passively captured into an operator log or audit trail, without the user taking any “action to sign.”
11.100(b)	177	Remove or clarify that the organization is looking to establish legal identity as a condition of hire per appropriate lawful requirements.	Companies take precautions to hire qualified, legitimate employees. Imposing this broad requirement at this regulatory level is burdensome while adding questionable value. In addition, non-organizational employees, such as contractors are not covered.
11.100(c)	188-190	Remove.	“Additional certification” as a stand alone item seems unnecessary. Proof of training on the obligations of using an electronic signature is adequate and does not need to be specifically required. Alternatively, a general statement that documented training shall be performed on the legal consequences of e-signature use may be acceptable substitute language.
11.200(a)(ii)(2)	206	Remove.	We believe this section is redundant.
11.200(a)(ii)(3)(b)	210-211	Remove.	The very nature of biometrics is based on unique, human physical characteristics. Validation should discern if they are configured in such a manner as to prevent circumvention.

Section	Paragraph Figure/ Table Line No.	Proposed Change	Comment/ Rationale
11.300	General Comment	Good computer system management mandates that password and ID combinations, whether e-sig or not, shall employ the same controls regarding assignment, availability, uniqueness, aging, risks to compromise. See Subpart C general comment.	We believe that discriminating between e-sig user IDs and passwords and "identity-only" user IDs and passwords is meaningless.
11.300(d)	231-234	Clarify "transaction safeguards."	Add use of timeouts, 3 strikes or other means as ways to minimize unauthorized use.
11.300(e)	236-237	Remove or modify to limit scope	Tokens or cards used for general network access have planned obsolescence and are constantly being "validated" against their own technology infrastructure. An IT organization that is providing token hardware and support has a stand-alone process for managing these devices. A token or device specifically being used to access a system directly should be tested during qualification of the system itself or treated as a "utility service" and qualified on its own merits.

Genzyme appreciates the opportunity to comment on and make suggestions for modifications to 21 CFR Part 11. Please contact me at (617) 768-6275 or Juliette Shih at (617) 768-6929 should you have any questions regarding this letter.

Cordially,



Alison Lawton
Senior Vice President
Regulatory Affairs



Juliette Shih
Manager, Operations Compliance
Biomedical and Regulatory Compliance