



Bristol-Myers Squibb Company

Joseph F. Lamendola, Ph.D.
Vice President
Global Regulatory Strategy
Pharmaceutical Research Institute

P. O. Box 4000 Princeton, NJ 08543-4000
Tel 609-252-3781 Fax 609-252-7781
Joseph.Lamendola@bms.com

December 17, 2004

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

Re: Docket No. 2004D-0440; Proposed Rule/Draft Guidance, *Draft Guidance for Industry on Computerized Systems Used in Clinical Trials*; 69 Federal Register 191 (October 4, 2004)

Dear Sir or Madam:

Bristol-Myers Squibb (BMS), a diversified worldwide health and personal care company with principal businesses in pharmaceuticals, infant formulas, and nutritional products, is pleased to have the opportunity to offer comments on the draft guidance. Our company's mission is to extend and enhance human life by providing the highest-quality pharmaceutical and related health care products. For this reason, we are interested in commenting on the *Draft Guidance for Industry on Computerized Systems Used in Clinical Trials*. Our comments are set forth below.

Summary of BMS Comments on Proposal

We commend the U.S. FDA for taking a leadership role in developing standards for the use and acceptance of electronic records and signatures. Such use has proven to be beneficial to both industry and FDA. We further commend the agency in its continued efforts to develop this guidance for *Computerized Systems Used in Clinical Trials*. In general, Bristol-Myers Squibb found the guidance to provide useful approaches to maintaining the quality and compliance of electronic records over their required retention period. Consistency with the *Part 11 Guidance – Scope and Application* document in acknowledging that hardware, operating systems, application software, and software development tools do not have to be retained to support reprocessing of data is excellent guidance. Furthermore, we also thought the consistency with the 1999 Guidance on Computer Systems Used in Clinical Trials regarding the fact that “clinical investigators are not generally responsible for validation unless they originated or modified the software” continues to be a practical and realistic approach to validation at clinical investigational sites. We strongly encourage the agency to continue its efforts in this direction and look forward to further implementation of the concepts contained within the *Part 11 Guidance – Scope and Application*.

Although the draft guidance is generally consistent with both the 1999 guidance of the same name and the recent Scope and Application document, the following comments summarize

2004D-0440

C8

ongoing concerns with the current approach to the effective use electronic records in a clinical setting. Challenges in applying the current guidance limits the practical use of electronic records in a clinical setting.

General Comments

A recurring issue for sponsors relates to ownership of source records after study completion and throughout the record retention period. This guidance does not speak to portability of electronic records that may be maintained by an institution after the investigator changes location. In addition, the guidance does not speak to ownership of records for the above mentioned situation. One example of this type of situation is the Veterans Health Administration system (VistA) whose original system architecture is now approximately 20 years old and has over 100 applications with potential for use in clinical research. When investigators leave the VA, clinical records maintained electronically, would most likely not be in a format accessible outside the VA network infrastructure. We recommend that the guidance clarify the Agency's expectation regarding responsibilities of the sponsor, CRO, and/or investigator throughout the record retention period, as defined by the predicate rules.

Throughout the document the Agency uses several terms such as "persons", "firms", various references to "site(s)", "regulated company's", etc. Consequently, obligations and/or responsibilities associated to a sponsor, CRO or investigator are not always easily discernible. For clarity, the guidance should more clearly identify specific obligations and/or responsibilities of the sponsor, clinical investigator, institution or CRO which are relevant to compliance with 21 CFR 312, 511, and/or 812.

Section VIII of the draft guidance provides guidance relative to the Agency's expectations on Security. However, several other sections within the document also reference topics/measures that would be generally classified as "security." We recommend that all topics that would fall under security be incorporated into section VIII.

Specific Comments

III.1 General Principles

In this section the agency recommends that "*each study protocol identify at which steps a computerized system will be used*". Due to the variety of systems available at clinical sites, adherence to this aspect of the guidance may not generally be feasible. Also, the intent and/or reason for identifying computerized systems used in each step of clinical trials in the study protocol is not clear, especially since section III.2 recommends identifying the actual systems used.

Recommendation: It is recommended that this expectation be removed from the guidance.

III.2 General Principles

This section of the draft guidance indicates that documentation of software and hardware used in a clinical trial should be retained as part of the study records. While we understand that this information should be on file at the system owner's location and available during the course of an inspection, it is not clear whether this information is intended to be maintained by the sponsor, CRO, or at the clinical site.

Recommendation: It is recommended that this expectation be clarified to indicate that system owners have a responsibility to maintain records of computer systems used in those aspects of a clinical study conducted under their control.

III.3 General Principles

This section of the draft guidance indicates that a system be designed to meet requirements defined within a study protocol. Computerized systems used in clinical trials are typically in place prior to starting a project and are not routinely designed for a specific study protocol. Rather, they are typically designed to meet the requirements of a variety of study designs.

Recommendation: It is recommended that this expectation be clarified to state that systems used in support of clinical trials should be of appropriate capacity and design for their intended use .

V. Standard Operating Procedures

This section refers to a list of SOPs to "*be available on site*". Although we support the agency in providing a guidance on the types of SOPs recommended for computerized systems, the appropriate location of these SOPs should be clarified. For applications maintained by the sponsor/CRO, an investigator site should not be required to maintain the entire set of procedures listed in the guidance. Only those SOPs relevant to activities being performed by the investigators and/or their staff should be required at the investigator site.

Recommendation: To clearly define the location of SOPs for computerized systems under the scope of this guidance it is recommended that SOPs only need to be maintained at sites responsible for conducting the activities addressed in the respective SOPs. Additionally, since validation is discussed elsewhere in the guidance, SOPs on validation would be expected, when validation of a system is expected.

VI.A Computer Access Controls

This section provides guidance regarding Agency expectations for control and administration of access controls for a computerized system. However, lines 164-165 which state "*We recommend that individuals not be allowed to log onto the system to provide another person*

access to the system” could imply that a system administrator should not be allowed to reset passwords for a user.

Recommendation: It is recommended that this statement be removed from the guidance as it is redundant (see statement in lines 163-164), “*We recommend that individuals work only under their own password or other access key and not share these with others*” and appears to provide no additional value.

VI.B Audit Trails or other Security Measures

The statement in lines 196-198 indicates expectations for investigators to maintain documentation created to track electronic records. It is not clear whether this applies to: (1) the systems for which they are responsible, or (2) all systems used for their data, including institutional systems, or (3) all of their data, including information from the sponsor or CRO. In addition, the draft guidance indicates that documents that track changes to electronic records should not be modifiable by users of the system. It is not clear how this would be accomplished for non-electronic records that track changes made to information that document activities related to the conduct of a clinical trial.

Recommendation: It is recommended that these statements be either clarified or removed from the document.

VI.C Date/Time Stamps

This section of the draft guidance recommends (lines 234 to 235) “*the ability to change the date or time should be limited to authorized personnel and such personnel should be notified if a system date or time discrepancy is detected*” and that changes to date and time should be documented. This may not be technically feasible for stand alone PC applications common in clinical research.

Recommendation: It is recommended that the guidance be revised to state the following: “*Where possible, the ability to change the system date or time should be limited to authorized personnel and such personnel should be notified if a system date or time discrepancy is detected. In lieu of system controls, this process should be controlled procedurally by the system owner.*”

VII.A Systems Used for Direct Entry of Data

This section of the guidance provides guidance on Agency’s expectations on system features that would aid in the consistent collection of clinical data into a computerized system. However, the final sentence in this section (lines 258 to 259), which states “*We recommend against the use of features that automatically enter data into a field when the field is bypassed*” could imply that the use of metadata and default values can not be used.

Appropriately designed, these features have been proven to increase accuracy and consistency in the data entry process in certain well controlled circumstances. System prompts are used document acceptance and to ensure that all data entered into the system are approved by the user at the time of entry.

Recommendation: It is recommended that this statement be clarified to allow for automatically entered data with appropriate acknowledgement by the user.

VIII. System Security

We have three comments pertaining to this section:

- For clarity, it is recommended the word “storing” in line 291 be changed to “securing”.
- Lines 308-309 indicate that the names of authorized personnel, their titles and their access privileges be available in study documentation at the site. It is not clear which site is being referenced in this section. It addition, it is not clear that value would be added by maintaining an entire list of individuals with access to a given system at an investigator site.

Recommendation: It is recommended that the guidance document be clarified to indicate that users and their respective access rights should be maintained and made available in the event of a regulatory inspection.

- Lines 314-315 indicate that if a computerized system is provided to an investigator by a sponsor, the study software should be “*logically and physically isolated as necessary to preclude unintended interaction with nonstudy software*”. It is not clear that this level of isolation is required or possible in all cases. Typically, these systems will have been validated and any interaction with nonstudy software would have been identified and resolved. Subsequent changes to the system should be evaluated by the responsible party as part of the ongoing change management process.

Recommendation: It is recommended that lines 314 and 315 be clarified to read “*If a computerized system being used for clinical trials operates on a computer shared for use with other systems, we recommend that efforts are made to identify and minimize unintended interaction between the systems.*”

IX. System Dependability

We support the Agency’s approach to validation of computerized systems using a documented risk based approach. However this section indicates that systems documentation (typically interpreted to include validation documents) and an “*overall description of the computerized systems and the relationships among hardware, software, and physical environment*” should be readily available at the site where clinical trials are conducted (lines 329-331). It appears as though the Agency is recommending additional copies of document(s)

be created, distributed and maintained which adds to the paperwork burden that already exists. The section also states that it is the “regulated company’s” responsibility to produce the validation documentation. This seems to be redundant if system documentation are expected to be maintained at the clinical site. As noted in the guidance, an investigator may be responsible for producing validation material if they originate or modify the system; however, maintaining systems and/or validation documentation at clinical sites would not be appropriate in cases in which the sponsor has responsibility for maintaining the system.

Recommendation: Clarification should be provided to indicate that systems and/or validation documentation are to be maintained by the organization responsible for the computer system and should be made available as required for regulatory inspections. Additionally, the phrase “regulated company’s” should be reconsidered to also include investigator sites, as necessary.

IX.B. Off-the-shelf Software

We have two comments pertaining to this section of the guidance:

- It may not be feasible to maintain vendor’s design level and/or original validation documents at each sponsor or contract research organization (CRO) site. Vendor evaluations are typically conducted as part of the QA program and as such results of these evaluations are considered QA records not typically provided for review in a regulatory inspection. Evidence of due diligence in the form of a quality program to assure that vendors employ adequate system development procedures should be demonstrated for off-the-shelf (OTS) software; however, sponsors should not be expected to maintain copies of vendors’ design level validation or to provide copies of their QA records in routine regulatory inspections.

Recommendation: Obligations of the Sponsor or CRO and Investigator should be clarified as they pertain to software vendors. It is recommended that this section be modified to clearly indicate the sponsor’s responsibility in “*demonstrating due diligence in assuring that OTS software was developed in accordance with industry standards and performs in a manner consistent with its intended use.*” It addition, it is recommend that references to “*original validation documents or on-site vendor audit documents*” be removed from the guidance.

- Lines 394-399 identify database and spreadsheet software as a special case for which the sponsor or CRO may not have documentation of design level validation and suggests that functional testing should be performed. As noted in the Scope and Application Guidance (as well as in this guidance starting on line 377), the sponsor should determine whether validation is required, based on (1) predicate rule requirements and/or (2) a documented and justified risk based assessment.

Recommendation: It is recommended for clarity that lines 394 to 399 be removed from the guidance as they appear contradictory and inconsistent with the current agency’s approach to conducting validation and system testing based on a justified and documented risk based on predicate rule requirements.

X. System Controls

We have two comments on this section of the guidance:

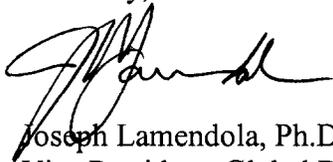
- Contingency Plans: It is not clear who would be responsible for ensuring written procedures for contingency plans for system failure.

Recommendation: Clarification should be provided to indicate that system contingency plans are to be maintained by the organization responsible for the computer system and should be made available to sites on an need basis and/or as required for regulatory inspections.

- The section (lines 430-434) pertains to ensuring that software version(s) are accurately identified in the system documentation. It is recommended that this expectation be removed from the System Controls section and included in Section III.2 which indicates that software and hardware should be identified in the study records.

BMS appreciates the opportunity to provide comment and respectfully requests that FDA give consideration to our recommendations. We would be pleased to provide additional pertinent information as may be requested.

Sincerely,



Joseph Lamendola, Ph.D.
Vice President, Global Regulatory Strategy