Guidance for Industry

Blood Establishment Computer System Validation in the User's Facility

Additional copies of this guidance are available from the Office of Communication, Outreach and Development (OCOD), (HFM-40), 1401 Rockville Pike, Suite 200N, Rockville, MD 20852-1448, or by calling 1-800-835-4709 or 301-827-1800, or e-mail ocod@fda.hhs.gov, or from the Internet at http://www.regulations.gov, or http://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/default.htm.

For questions on the content of this guidance, contact OCOD at the phone numbers or e-mail address listed above.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Biologics Evaluation and Research
April 2013

Table of Contents

Contains Nonbinding Recommendations

Guidance for Industry

Blood Establishment Computer System Validation in the User's Facility

This guidance represents 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 appropriate FDA staff. If you cannot identify the appropriate FDA staff, call the appropriate number listed on the title page of this guidance.

I. INTRODUCTION

We, FDA, are issuing this guidance to assist you, blood establishments, in developing a blood establishment computer system validation program, consistent with recognized principles of software validation, quality assurance, and current good software engineering practices. This guidance addresses a blood establishment's validation of its Blood Establishment Computer *System* (system) which incorporates Blood Establishment Computer *Software* (BECS). In the context of this guidance, the term "user's facility" means the blood establishment.

This guidance describes the following:

- Requirements in Title 21 Code of Federal Regulations (21 CFR) (e.g., 21 CFR 211.68, 606.100(b), and 606.160) that apply to blood establishment validation of systems; and
- FDA's recommendations for the validation of systems.

While this guidance may provide manufacturers of BECS with information about validation of computer systems in the user's facility, this guidance does not address the software manufacturer's validation responsibilities, or the submission of a 510(k) premarket notification for BECS. For guidance on validation applicable to the manufacturer of medical device software, including BECS, see the FDA guidance document entitled, "General Principles of Software Validation: Final Guidance for Industry and FDA Staff" dated January 2002 (Ref. 1). For guidance on the submission of a 510(k) for BECS, see the FDA guidance document entitled "Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices" dated May 2005 (Ref. 2).

This guidance finalizes the draft guidance entitled "Guidance for Industry: Blood Establishment Computer System Validation in the User's Facility" dated October 2007.

FDA's guidance documents, including this guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the FDA's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited.

The use of the word *should* in FDA guidances means that something is suggested or recommended, but not required.

II. BACKGROUND

A. Description of Blood Establishment Computer System

A Blood Establishment Computer System (system) includes: computer hardware; computer software; peripheral devices; networks; personnel; and documentation, e.g., User's Manuals and Standard Operating Procedures (SOPs). The computer software used in a system includes BECS, which is a medical device. Systems also are regulated as equipment under 21 CFR Part 606 (Current Good Manufacturing Practice for Blood and Blood Components), specifically 21 CFR 606.60, and as automated or electronic equipment under 21 CFR Part 211, Subpart D (Equipment), specifically 21 CFR 211.68.

B. Description of Blood Establishment Computer Software

BECS is software designed to be used in a blood establishment and is intended for use in the diagnosis of disease or other conditions in donors, or in the prevention of disease in humans by preventing the release of unsuitable blood and blood components. Some of the intended uses of BECS include:

- Use during the manufacturing process for determining donor eligibility and release of the blood or blood component as suitable for transfusion or further manufacture;
- Use in transfusion services to perform compatibility testing and other related functions;
- Use to establish positive patient identification prior to transfusion by scanning machine readable information such as barcodes on patient wristbands (or other electronic data storage items), specimen containers, and blood product labels; and
- Use to perform other functions associated with transfusion, such as recording patient vital signs and tracking blood products.

C. Definitions and Terminology

In addition to the following definitions used in this guidance, you may find other terms relating to systems and BECS in the FDA Glossary of Computer Systems Software Development Terminology (Ref. 3). The use of some terms in this guidance or in FDA regulations may vary somewhat from some uses in industry. For example, both FDA and the International Organization for Standardization (ISO 8402:1994) regard "verification" and "validation" as separate and distinct terms. However, many software engineering journals and textbooks use the terms "verification" and "validation" interchangeably, or in some cases, refer to software "verification, validation, and testing (VV&T)" as a single concept, with no distinction among the three terms. We provide the following definitions

in an effort to clarify our meaning of specific terms where our usage may vary somewhat from some uses in industry.

Qualification operational means establishing confidence that process equipment and sub-systems are capable of consistently operating within established limits and tolerances (Ref. 3).

Risk assessment means a comprehensive evaluation of the risk and its associated impact (Ref. 3).

Software regression testing means re-running test cases which a program has previously executed correctly to detect errors caused by changes or corrections made during software development (Ref. 1).

Software validation means confirmation by examination and provision of objective evidence that the particular requirements for the software's intended uses can be consistently fulfilled (Ref. 1).

Software verification means confirmation by examination and provision of objective evidence that specified requirements have been fulfilled (Ref. 1). In a software development or manufacturing environment, software verification provides objective evidence that the design outputs of a particular phase of the software development life cycle meet all of the specified requirements for that phase.

User validation means testing new equipment or a new process in the environment where it will be used to ensure that it will reliably produce a product that meets pre-determined qualifications and quality standards (Ref. 4).

III. DISCUSSION

A. Vendor Selection for BECS

While not strictly part of system validation, we recommend that you evaluate and compare the available BECS with the needs of your blood establishment and select a BECS that meets your requirements. We further recommend that you monitor reports of adverse events and recalls applicable to your BECS (Refs. 5 through 9).

We provide a list of 510(k) cleared BECS on our web site (Ref. 9). You should note that the version number listed is the version that received clearance; however, the manufacturer may have released an upgrade that did not require a new 510(k) clearance. You also should note that the list on our website is cumulative and may include BECS that may no longer be available or supported by the original manufacturer.

B. System Documentation

You must maintain documentation for your system (21 CFR 211.68, 211.100(a), 606.100(b)(15), 606.160(b)(5)). You should ensure that the documentation is current, accurate, and as detailed as necessary to ensure proper use and operation of the system. We recommend you include, but not necessarily limit, the documentation you maintain to the following, as applicable to your blood establishment:

- Information available from the software developer, such as:
    - Hardware specifications and hardware requirements;
    - Instruction manuals, e.g., User's Manual, Operations Manual, Installation Manual, System Administration Manual, etc.;
    - Environmental requirements;
    - Network diagram;
    - System description;
    - List and location of peripheral devices such as printers and terminals;
    - Processor type(s);
    - Operating system and version number;
    - System memory;
    - Disk configuration;
    - Type and location of backup media;
    - List of interfaces; and
    - List of environments on system, e.g., test, training, production, etc.

- Information available from the system administrator, such as:
    - Validation records;
    - Record of hardware and software maintenance, including date performed;
    - Record of changes made to the system hardware, software and peripheral devices, including date;
    - User training records;
    - SOPs; and
    - Problem reports and their resolution.

Note: Although a remote access log is not part of validation records, you may consider keeping a log of remote access to any part of your system, such as the BECS or laboratory instruments. We recommend this log include the date, time, reason for the access and the name of the person connecting to your system.

C. Validation Plan

Before you start user validation, you must define and control how you will validate the system through the use of a written plan designed to assure proper performance (21 CFR 211.68(a)). A written plan is not "designed to assure proper performance" unless it requires user validation prior to routine use, on a routine basis, and any time a change is made that has the potential to affect the functions of the system. In addition, input to and output from the system must be checked for accuracy (21 CFR 211.68(b)). Therefore, before you start validation, you must develop a validation protocol and acceptance criteria to ensure the system is performing properly (21 CFR 211.68(a)).

The validation plan defines "what" the validation effort should cover. Validation plans specify areas such as scope, approach, resources, schedules, training, the types and extent of activities, tasks, and work items, identification and resolution of software defects/bugs or anomalies, responsibility and the approval process (Ref. 1).

D. Scope of Validation

Your activities should assure that the system components have been validated and are suitable for your specific operations and workload and can accurately and repeatedly meet your needs (as defined in your requirements documents). You should validate your system at your location using the same software, hardware, SOPs, and personnel who will use the system after it is formally implemented. Thus, in cases where a central server is used by multiple locations, not only the main server but also each individual location should have a validation plan that is specific to the functions and configurations at each location. Equipment vendors may provide assistance for equipment qualification and consultants may provide assistance with the validation project. However, you are ultimately responsible for validation of your system in your facility.

Validation of your BECS falls under your Current Good Manufacturing Practice (cGMP) requirements and should reflect and anticipate the BECS' actual use in your establishment. We recognize that it is a common practice for software manufacturers to provide test cases to blood establishments for use in system validation. We recommend that you carefully assess the software manufacturer's test cases, consider your own intended use of the software, your internal policies and procedures, and add or change test plans as appropriate to ensure that the software will accurately and repeatedly meet your requirements. The test cases should include those that represent "worst case scenarios," e.g., maximum numbers of users working simultaneously, all possible activities occurring simultaneously, etc.

We recognize that BECS validation is difficult because you cannot test indefinitely, and it is hard to determine how much evidence is sufficient. Generally, software validation is a matter of developing a "level of confidence" (Ref. 1) that the software device meets all requirements and user expectations for the automated functions and features of the software.

E. Risk Assessment

The level of confidence and, therefore, the level of validation effort needed, varies depending upon the potential hazards posed by the automated functions of the system. Your test plan and test cases should be developed based on a risk assessment. We, therefore, recommend that you perform a risk assessment early in the validation process. After performing that assessment, you should determine the degree of validation necessary based on the identified risks, and then develop your test plan and test cases accordingly. The highest risk functions of the system should be tested more comprehensively. For example, because of the potentially fatal consequences of a transfusion based on an improper crossmatch between donor and recipient, the validation of the electronic or computer crossmatch would require more extensive testing.

Because of the complexity of software, especially BECS, it is difficult to predict the probability of a hazard occurrence. Therefore, when you conduct your risk assessment, we recommend you consider most hazards to have a high probability of occurrence.

F. Validation Procedures

You must develop SOPs for your validation activities as required by 21 CFR 211.68(a), 211.100(a), and 606.100(b)(15). We recommend that your validation SOPs include, but not necessarily be limited to, the following:

- Writing a validation plan;
- Performing system maintenance;
- Performing a risk assessment;
- Writing a validation report;
- Addressing change control;
- Writing test cases;
- Amending test cases;
- Handling validation deviations; and
- Validating after a change.

G. Validation Activities

Consider the following points as you prepare to perform validation activities:

- We recommend that you perform validation in the "test environment" or "test partition" of your system. After successful validation, you or your software manufacturer should copy or move the file configuration on which you performed your validation into the production environment.
- Each executed test case in your pre-defined written test plan should include the input, expected output, actual output, acceptance criteria, whether the test passed or failed, the name or initials of the person performing the test, and the date the test was performed. Test cases should include normal results (results within the

"normal" range), abnormal results (unacceptable results or those outside the "normal" range) and boundary results or values. Boundary testing is testing at the boundary of a specification, in other words, at the limit, just below the limit, and just over the limit. Boundary values are "off-by-one errors." An example of boundary testing is testing for a hematocrit of 37%, 38% and 39% if the cutoff (or boundary value) for hematocrit is 38%. You should also test for "absurd" results (invalid or nonsense results). Examples of absurd or unexpected values might be an alpha result in a numeric field, a hematocrit of 110% or a blank (or leading blank) in a result field.

- You must retain validation records (21 CFR 211.68(b), 211.100(b), 606.160(b)(5)(ii)). Your records should include documented evidence of all test cases, test input data and test results. Test results should include screen prints. For traceability purposes and to facilitate quality assurance review and follow-up, we recommend that any supporting documentation, such as screen-prints, where appropriate, be identified to link them to the specific test case.
- We recommend that you test at simulated peak production times in an appropriately sized test environment and with the maximum number of concurrent users to assure proper system performance.
- We recommend that you test to assure you have correctly defined system security and that all users can log on with the correct security privileges.
- We recommend that you qualify equipment, validate all interfaces, including those to a Hospital Information System (HIS) (e.g., admissions, discharges and transfers (ADT)); a Laboratory Information System (LIS) (e.g., order entry/results return (OE/RR)); and all instrument interfaces, as applicable. Monitoring of interface error files should continue subsequent to implementation as unforeseen transaction types or data elements may cause disastrous results (for instance, orders not being received, results posting to the incorrect donor/patient record, etc.).
- You must train personnel in the use of the system procedures (21 CFR 211.25(a), 600.10(b), 606.20(b)). Training should include assessing an individual's ability to understand and correctly use the system. You should evaluate your personnel's ability to perform system maintenance procedures, such as backups, and their ability to respond in an appropriate and timely manner to all alarms, warnings and error messages.
- We recommend that you verify the output of system reports. We recommend you include any reports containing donor or recipient history information, product quarantine reports, donor or patient merge reports, and patient chart reports (as applicable) in this effort. It is particularly important to ensure that reports print in lower and upper case if the system keeps records of red blood cell phenotype or antibodies.
- We recommend that you closely monitor the system for a period of time after installation of the new or upgraded software in the production environment to detect any discrepancies that were not identified by the test cases.
- If your system includes the use of wireless radio frequency (RF) technology, we recommend that you evaluate the device for wireless coexistence, performance,

data integrity, security, electromagnetic compatibility (EMC), and electromagnetic interference (EMI) in the setting in which you will use it. For further information, see the FDA draft guidance document entitled, "Draft Guidance for Industry and FDA Staff, Radio-Frequency Wireless Technology in Medical Devices" (Ref. 10). When finalized, this draft guidance will represent FDA's current thinking on this topic.

- Although not a function of your system, we recommend that you validate the data conversion from your legacy system to your new system to avoid problems such as duplicate donor records and deferral codes.

H. Validation Report

You must document your validation activities pursuant to 21 CFR 211.68, 211.100(b), and 606.160(b)(5). Your validation report should include a summary of the test results, including any variances or failed tests, any amendments made to the test cases or the validation plan, an evaluation of the outcome of your testing, and approvals or sign-offs by management, including dates.

I. Validation after a Change

When the BECS manufacturer modifies the software, the manufacturer should inform you of other functions that might be affected. We recommend that your contract with a software manufacturer specifically address this issue. However, you are ultimately responsible for assuring that the system used in your establishment has been validated for use in your establishment.

Due to the complexity of systems and BECS, a seemingly small local change (e.g., software, hardware, peripherals, or infrastructure) may have a significant global system effect. When any change (even a small change) is made to the software on the system, a software regression analysis should be conducted, not just for validation of the individual change, but also to determine the extent and impact of that change on the entire system. Based on the analysis, you should then conduct an appropriate level of software regression testing to show that unchanged but vulnerable portions of the system have not been adversely affected. Appropriate regression analysis and testing provide the confidence that the system is validated after a software change (Ref. 2). We recommend that you perform regression testing, when indicated by your analysis, by re-running test cases that previously passed.

J. Integrated Package vs. Stand-Alone

If your system or BECS is part of an integrated package on a Laboratory Information System (LIS) or Hospital Information System (HIS) rather than a stand-alone system, you should also consider how changes made to functionality shared by the LIS or HIS and BECS (such as ADT, orders, etc.) might affect your system or BECS. You should determine what functions or files your LIS or HIS and your BECS share by discussing this with your BECS manufacturer.

IV. REFERENCES

1. General Principles of Software Validation: Final Guidance for Industry and FDA Staff (January 11, 2002), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085281.htm.

2. Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (May 11, 2005), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm.

3. FDA Glossary of Computer Systems Software Development Terminology, (8/95) http://www.fda.gov/ICECI/Inspections/InspectionGuides/ucm074875.htm.

4. Guidance for Industry: "Computer Crossmatch" (Computerized Analysis of the Compatibility between the Donor's Cell Type and the Recipient's Serum or Plasma Type) (April 2011) http://www.fda.gov/downloads/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/Blood/UCM252894.pdf.

5. Warning Letters http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/default.htm.

6. Adverse Event Reports (Maude Database), http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/textsearch.cfm.

7. FDA Enforcement Reports Index, http://www.fda.gov/safety/recalls/enforcementreports/default.htm.

8 Recalls, Market Withdrawals and Safety Alerts, http://www.fda.gov/Safety/Recalls/default.htm.

9. 510(k) Blood Establishment Computer Software, http://www.fda.gov/BiologicsBloodVaccines/BloodBloodProducts/ApprovedProducts/SubstantiallyEquivalent510kDeviceInformation/ucm134987.htm.

10. Draft Guidance for Industry and FDA Staff, Radio-Frequency Wireless Technology in Medical Devices (draft released for comment on January 3, 2007), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077210.htm.