[Docket No. 93N-0394]

Draft Guideline for the Validation of Blood Establishment Computer Systems

Prepared September 28, 1993

TABLE OF CONTEHTS

I. PURPOSE

The purpose of this guideline is to assist manufacturers of blood and blood components, including blood banks and plasmapheresis centers, in developing a computerized system validation program consistent with recognized principles of system development methodology and quality assurance that are current good manufacturing practices. This is not intended to be a guideline for software manufacturers who may be subject to other guidance and requirements.

II. SCOPE

This guideline may be useful to blood establishments in developing and administering a computerized system validation program. Because the Food and Drug Administration (FDA) is in the process of revising 21 CFR 10.90(b), this document is not being issued under the authority of 21 CFR 10.90(b), and the document, although called a guideline, does not bind the agency and does not create or confer any rights, privileges, or benefits for or on any person. Blood establishments may follow the guideline or may choose to use alternative procedures not provided in the guideline. If a blood establishment chooses to use alternative procedures, the establishment may wish to discuss the matter further with the agency to prevent expenditure of resources on activities that may be unacceptable to the Food and Drug Administration (FDA).

Blood, blood components, or derivatives applicable to the prevention, treatment, or cure of human diseases or injuries are specifically identified as biological products subject to regulation pursuant to the Public Health Service (PHS) Act [42 U.S.C. 262, section 351 (a) (1)]. Similarly, blood, blood components, or derivatives intended for use in the diagnosis, cure, mitigation, treatment, and prevention of diseases in humans are drugs as defined in section 201 (g) of the Federal Food, Drug, and Cosmetic (FD&C) Act [21 U.S.C. 321 (g)]. section 501 (a) (2) (B) of the FD&C Act states, in part, that a drug shall be deemed to be adulterated if "the methods used in, or the facilities or controls used for, its manufacture, processing, packing, and holding do not conform to, or are not operated or administered in conformity with, current good manufacturing practice to assure that such drug meets the requirements of the FD&C Act." Because blood and blood components are defined as drugs in the FD&C Act, the Current Good Manufacturing Practices (cGMP) in 21 CFR, Parts 210 and 211, are applicable. This guideline is intended to be used in conjunction with the applicable federal standards in 21 CFR, Parts 600 through 680, and Parts 210 and 211, as they pertain to biological products for human use. Note that sections 210.2(a) and (b) provide that where it is impossible to comply with the applicable regulations in both Parts 600 through 680 and Parts 210 through 211, the regulation specifically applicable to the product shall apply and supersede the more general regulation. Applicable regulations may be found in Section XIV. A. and Section XVII. of this document.

The agency may amend this guideline after receiving comments submitted by interested persons, and as necessary thereafter.

III. INTRODUCTION

Blood establishments (e.g., blood banks, blood product testing laboratories, plasmapheresis centers, and transfusion services) have rapidly expanded the use of computers as tools in the manufacture of blood and blood components to assist in decision-making and in the management of critical data (e.g., donor registry, laboratory testing, storage of required records and data).

Proper performance and use of computerized systems in the manufacturing process is a critical part of final product quality. Blood establishments currently using and those considering use of computerized systems should clearly understand the need to establish and define the functions to be performed by the computerized system, the way in which it will interact with both manual and automated operations, and the importance of data integrity.[1]

This document provides general guidance on the process of validation of computerized systems used in blood establishments. The goal of validation is to perform and document systematic procedures that give assurance that the computerized system is functioning as specified and intended at each user site, including existing and new installations, and after every significant system change.

This document should also be useful for the hardware and software vendors that supply products used as key components of the blood establishment's computerized systems. By understanding the regulatory needs of the blood establishments, hardware and software vendors can better define the features, capabilities, and limitations of their products.

This document supersedes the information provided in the April 6, 1988, and September 8, 1989, memoranda regarding the use of computerized systems in registered blood establishments (see Section XIV. C. Memoranda).

Licensed blood establishments are reminded that they are required to report the proposed installation or major modification of a computerized system if it is to be used in the manufacture of blood and blood components to the Director, Center for Biologics Evaluation and Research (CBER), as a supplement to the firm's establishment license application (ELA) (see Section XIII. Reporting to CBER).[2]

IV. COMPUTERIZED SYSTEM DEFINITION

A blood establishment's computerized system includes: hardware, software, peripheral devices, personnel, and documentation [e.g., User's Manual, Standard Operating Procedure (SOP)]. Defining the computerized system logically begins by first documenting the user's needs and requirements. This also helps avoid misunderstanding between the user and the developer. The user should work with the system developer to define all steps in each function to be performed by the computerized system. The requirements should include a written description of the tasks to be performed including compliance with local, state, and federal regulations. If the computerized system is not defined in terms of components and functions, a well designed validation program can not be established.

A. System Components

The development of a computerized system should include all the specifications for each of the system's components (e.g., parameters, limitations, and constraints). The user of the computerized system should account for operational needs and requirements, as well as establishing criteria for personnel training and quality assurance to ensure the consistent and reliable performance of the system in the working environment.[3]

Hardware, software, and peripheral device factors include:

- the compatibility between the hardware and software,
- the interfaces with peripheral devices,
- the physical constraints (e.g., space, power, air conditioning requirements, electromagnetic and radio frequency noise or interference, etc.), and
- maintenance and calibration procedures.

Personnel factors include:

- training,
- certification,
- unique identification,
- access limitations, and
- operating instructions (e.g., User's Manual, SOP).

The functions of the computerized system should be established with written descriptions outlining:

- inputs,
- processing,
- outputs,
- search criteria,
- data manipulation,
- data output format and content,
- structure of the database {e.g., definition of the fields and their contents), and
- communications with other equipment.[4]

B. System Documentation

The user should ensure that the documentation for the computerized system is current, accurate, and as detailed as necessary to ensure proper use and operation.[5] System documentation should include:

Vendor provided items, such as:

- operational specifications and requirements,
- instruction manuals [e.g., User's Manual, Operations Manual, Training Manual, (if the user will be maintaining the software, a program maintenance manual and other references .are also needed)],
- diagrams, flow charts, and descriptions that define the interactions between modules, for software (including interfaces),
- and test databases.

User provided items, such as:

- user's requirements,
- Standard Operating Procedures (SOPs),
- the test database and a description of the test cases,
- records of operational validation of integrated hardware, software, and peripheral devices, and
- records of maintenance and changes made to system hardware, software, and peripheral devices.

V. SYSTEM VALIDAXION PROTOCOLS

Validation is an essential component in the development and operation of a computerized system. A validation protocol is a written plan that is intended to be followed in testing a specific portion of the system or the total system in order to produce documented evidence that the system operates consistently and reliably. Validation protocols should be developed using system development methodology (SDM). SDM is a structured method used to plan, design, validate, and implement a system. SDM also incorporates the concepts and principles of quality control, quality assurance, and current good manufacturing practices (cGMP).

At a minimum, system validation protocols should include:

- a description of the function(s) to be tested,
- steps to be performed,
- equipment and methods to be used,
- inputs (from all sources), and
- expected outputs and evaluation criteria.

Documentation of the performance of the validation protocols and an analysis of the results should be maintained by the blood establishment.[6] Blood establishments, as manufacturers of biological products, are responsible for ensuring the proper operation and validation for all procedures performed and supported by the computerized system relating to the manufacture and distribution of blood and blood components. Blood establishments also should ensure that SOPs include how the computerized system is used during manufacturing steps and that these procedures conform to current regulations (21 CFR, Parts 600 through 660 and Part 211).

Vendors or developers that commercially distribute software intended for use by blood establishments should be aware of the federal regulations relating to the manufacture of blood and blood components. In addition, because blood bank software products are devices, firms manufacturing and distributing such products must comply with statutory and regulatory requirements applicable to devices.

A. Software Development

Blood bank software products are medical devices. The user should ensure that vendors supply specifications, documentation, and validation for each feature and function of the software product, including:

- data inputs and outputs,
- data manipulation within each module,
- module to module interaction,
- interaction with peripheral devices,
- data storage and maintenance (including back-up procedures), and
- data search and retrieval algorithms.

The user should ensure that software vendor(s) provide information concerning product features and limitations for use in the development of computerized system validation protocols and ensure that:

- the software was developed and validated by qualified persons using SDM,
- all versions of the software are kept in readable form (including source code),
- information will be provided to an FDA Investigator upon request,
- software modifications have and will follow a systematic change control cycle,
- notification will be provided concerning known design defects or operational errors, and
- provisions have been made for providing information to the user in instances involving interruption or cessation of the vendor's business.

B. User Responsibilities

Blood establishments as users should define the requirements for the system and establishing a written validation program that includes:

- system validation protocols,
- types of testing,
- detailed test cases,
- test database,
- documented results,
- documented evaluation and acceptance,
- schedule for periodic system evaluation, and
- revalidation as necessary.

When a new computerized system is being developed, close contact should be maintained between the blood establishment and the vendor(s) to gather information that may affect the system.

C. Blood Establishment As Software Developer

During inspections of blood establishments, three basic categories of software have been observed: 1) vendor supplied, 2) vendor Supplied/"in-house" modified, and 3) "in-house" developed. Irrespective of the source of the software, the developer should follow accepted standards for software development (SDM) including, but not limited to, proper design, software validation and verification procedures, change control, and detailed documentation.

Blood establishments are responsible for the quality of the software and validation of its design and features if they modify vendor supplied software or develop software in-house. Due to the impact of any change on the proper operation and functioning of the software, modification and development should only be performed by qualified individuals. The software developer should be aware of the contents of the Technical Report on Software Development Activities (1987), Reviewer Guidance for Computer Controlled Medical Devices (1991) and other agency documents, which provide guidance concerning software product development and validation.

D. Prospective System Validation and Revalidation

The user, after appropriate consultation with the vendor(s), should design a plan for the prospective validation of the computerized system. Written procedures for production and process controls must be established and followed to ensure that products produced will meet specifications.[7] Validation includes defining all components of the system, testing each component of the system, and testing integrated components of the system to ensure that pre-determined specifications are met (see Guideline on General Principles of Process Validation). Prospective validation is performed by the user prior to implementation of the computerized system in manufacturing operations. Prospective validation is performed for all new systems and before changes, modifications, or enhancements to existing systems which may affect finished product characteristics.

The routine revalidation of existing computerized systems parallels the validation of new systems. Routine revalidation is based on the protocols that are used for the prospective validation and is performed regularly after the installation of the system.

E. Retrospective Validation

Retrospective validation is described in the FDA's "Guideline on General Principles of Process Validation" {see section XIV. B. Food and Drug Administration Publications} It is extremely difficult to "retrospectively" validate a computerized system and is generally more costly and time consuming than prospective validation. If it must be attempted, significant information can be obtained through observation, documentation, and performance history. Generally, retrospective validation should be used only as a corrective measure in response to deficiencies noted concerning prior validation efforts.

For retrospective validation, the User's Manual, Operators Manual, Program Maintenance Manual, and the Training Manual provided by the vendor{s} will help to provide the general structure of the system. The blood establishment's SOPs should identify the tasks {including all steps} that are performed with the aid of the computerized system. Blood establishment personnel {or consultants} responsible for designing test cases can avoid making assumptions about the system functions if this documentation is complete. Missing or incomplete information may be reconstructed by researching:

- assembly specifications,
- maintenance logs, change logs, and records,
- project files,
- source code,
- software structure and data flow diagrams,
- computerized system test results {if any},
- previous versions of software, and
- failure reports.

F. Documentation

Computerized systems used in the processing and/or distribution of blood and blood components should have validation documentation that shows that the intended functions will consistently be performed accurately and reliably.[8] Documentation of validation includes:

- records demonstrating that the system met its predetermined specifications and requirements throughout development,
- records describing in detail the system's intended functions,
- records of testing {including all results} to demonstrate that the intended functions performed as designed during acceptance testing, and
- records documenting that hardware and software change controls are being followed as described.

VI. COMPUTERIZED SYSTEM TESTING

Evaluation of the system should be performed continuously to ensure that the hardware {including all peripherals) and system software {applications and the operating system) are operating as specified and that no unauthorized changes have been made. The user should ensure that the computerized system and the peripheral devices are being used in a manner that is consistent with their design. In addition, the user should ensure that the computerized system and the peripheral devices are calibrated in accordance with the equipment manufacturer's directions for use[9]. To evaluate the system, tests should be performed at the time of installation, after a change has been made, and on a routine basis according to schedules defined in the establishment's SOPs. Tests are an indispensable tool of validation.

Test case design should include normal inputs, boundary values, invalid inputs, stress conditions, and special cases. Properly analyzed test data are useful to identify additional testing needs, and the need to establish additional manufacturing control procedures {e.g., "work-arounds"). The test data will also be useful in establishing and documenting the repeatable and reliable performance of the computerized system.

> **CAUTION: Because the inteqrity of the data cannot be assured, system change/modification/enhancement testinq should ONLY be performed using a TEST database.**

Avoid the use of PASS/FAIL notation in the evaluation of the results of any type of testing. Actual test data, including inputs and test results, should be documented and available for review. PASS/FAIL notation is documentation of an interpretation which cannot be audited.

A. Testing Types

Software tests are intended to challenge the application software and other parts of the overall system functionally and structurally. Functional testing demonstrates only that the system outputs appear to be correct. It does not allow an assessment of whether the software is actually performing according to specifications and requirements. A complete functional test of every combination of inputs may not be feasible except for very small programs. Functional testing is essentially a subset of structural testing.

Structural testing should be designed to exercise all modules and branches of the software and their interrelationships with the hardware and peripheral devices. Structural testing should be performed to ensure that all relevant functions in the software perform as intended.

Each of the testing types described below should be conducted. Performing only one type of test will not prove that the system is working properly.

1. Normal Testing includes cases that test the functional and structural integrity of the computerized system. The input data for these test cases all fall within the range the user considers to be normal. Performing enough test cases can give a reasonable level of confidence that the system behaves as intended under normal conditions.

2. Boundary Testing is performed using values that force the system to discern whether the input *is* valid or invalid, or to make a decision as to which branch of the program to execute. Boundary test values are set at the edges (i.e., slightly below and above) of valid input ranges. Boundary testing does not mean making the computerized system "crash" or involuntarily stop.

3. Invalid Case Testing checks for input errors. The user should not assume that the system will detect invalid inputs. Invalid case testing demonstrates that, when the inputs are invalid values, the computerized system performs properly. Invalid inputs could be from the keyboard or from a peripheral device. Transposition or spelling errors are among the most common errors.

Electrical interference, line noise, conversion of analog into digital data, or a software fault could cause the input data to be in error.

4. Stress Testing challenges the computerized system at its physical limits and documents its continued ability to perform correctly. Stress testing includes situations where the computerized system, peripheral devices, and operators are pushed to the operational limits of the system or worst case scenario.

5. Special Case Testing, also known as "exceptional case testing", documents the system1s reactions to specific types of data or lack of data and is intended to ensure that the computerized system does not accept unsuitable data. These tests should be designed to document what happens when values that are not included in the ranges defined in the specifications are entered. Use of test cases with no data entry in a field will assist in establishing software system defaults. Special test cases should also challenge the system to determine if more than one person can add or edit important data at the same time, and if so, document how the system responds.

6. Parallel Testing is one of the most common types of tests performed by blood establishments. Parallel testing is performed by running two systems in parallel and comparing the outputs (e.g., two software application versions or software compared with a manual procedure). Modified software is often installed on the same physical drive as the production software, but in a separate region or partition. The parallel or test region system should emulate the production system except for authorized changes.

As commonly performed, parallel testing is not a completely effective form of functional testing because it focuses only on the cases presented during normal test runs; therefore, it checks only a narrow range of values. The design of parallel test cases does not always include invalid or boundary values. And, many times, the output is not properly analyzed. The comparison of the actual outputs to the predicted outputs is one analysis component frequently absent in the design of parallel testing plans.

> **NOTE: Due to the above, parallel testing cannot be relied upon as the sole criterion for validating a system. However, parallel testing I can be a valuable tool when it is used in conjunction with other testing types for validation, or to train personnel to use the new computerized system.**

7. Vendor Simulations may be performed by the developer, vendor or a third party to test a prototype or a simulation [e.g., ALPHA (developer's site) or BETA (selected user site) testing. Vendor simulations are not a substitute for validation by the user. Vendor simulations cannot completely emulate the user's environment or the people that will be using the system. Installing the computerized system in a different environment can cause changes in the system's operation. Because of the possibility of changes in the system's operation, testing at the time of installation should be performed by the user at each site, prior to approval and implementation.[10]

B. System Validation

System validation is based on test cases designed to verify and challenge the user's requirements, the system specifications, and the User's, Operations, and Maintenance Manuals. Analysis of the test data and an understanding of the system's structure should point out the need for other test cases required to complete testing. The user should determine and justify how many times each function should be tested. The criticality of the function will dictate the number and types of tests performed and the frequency of retesting and evaluation. Testing is complete when it has been demonstrated that the system repeatedly performs its intended functions and does not perform unintended functions.

The completion of validation, including an evaluation and summary of the test cases, the test data, the test database, and the results of testing should be approved through a formal process prior to implementation of the system or changes.[11]

C. Validation Documentation

Documentation of the validation process should reflect the tests and their results.[12] The SOPs should clearly define the protocol for each of the different types of systems tests. The documentation produced by good test plans will show that the system is running properly. At a minimum, validation protocols should document that:

- there are no unacceptable records,
- donor identification codes match the correct data,
- donor deferral codes are properly assigned and used,
- all units/components are properly identified,
- test results (including repeat tests) are properly entered and recorded,
- records of change (including audit trails} are correct,
- recorded and printed outputs are correct,
- manipulations and calculations are accurate and use the prescribed data,
- expiration dates are properly calculated, and
- video displays are correct.

VII. CHANGE CONTROL AND AUDIT TRAIL RECORDS

All changes that are made to the computerized system should be documented and formally authorized. Records of changes should include modifications and/or enhancements made to the hardware, software, and any other critical component of the system. The SOPs should clearly define the need for documentation of changes, an evaluation of the impact of a change, and an assessment concerning the necessity for revalidating portions or all of the system. It is recommended that changes to the computer hardware, software (including operating systems and interfaces), and peripheral devices be kept in separate logs.

Detailed records should be maintained for all hardware and software changes that are made to the system (e.g., corrections, modifications, upgrades, enhancements, etc.}. At a minimum, these records should include:

- a description of the change,
- a description of the tasks performed to effect the change date,
- person performing the task,
- equipment identification or modules that are affected,
- authorization signature,
- validation protocols,
- validation results, and
- documentation of approval and acceptance.

An audit trail documents changes made to the data. Audit trail records are part of the system's documentation and should only be accessible or reviewed by authorized persons {e.g., identified establishment personnel, FDA Investigators). Audit trails can be used to record access to the system. Each time an authorized or unauthorized user tries or gains access to the system there should be a log entry. At a minimum, an audit trail should include:

- the name of the person making the change,
- date,
- time,
- field name,
- previous data,
- and current data.

Changes to data may not obscure the original data.

VIII. MANUALS

A. Standard Operating Procedures (SOPs)

Standard Operating Procedures {SOPs) are procedural manuals that delineate the steps required to perform tasks. SOPs are the written "back-bone" of the blood establishment's operation. The SOPs should cross reference any vendor supplied documentation concern1ng 1nstructions for use.

The SOPs should include the procedures for handling all operations.[13] These operations range from normal events to the total recovery from any type of disaster {including but not limited to system failure or crash, power outage, natural disaster, etc.). Particular attention should be paid to the procedures for archiving {backing up) the data. These procedures should include all administrative, routine, and emergency situations, such as:

- detailed descriptions of all validation protocols and records of their results,
- roles of the systems and maintenance personnel,

- detailed descriptions of all catastrophic validation routines and records of their results, and,
- a complete disaster plan that describes the roles of all the facility's personnel.

Recovery from disasters should be a key concern. The methods and the location to be used for off-site storage of the archive should be carefully considered. Recovery procedures should define the responsibilities of all personnel during and while recovering from disasters. Disaster SOPs should include detailed descriptions, or cross-reference the locations, of:

- all validation procedures and records,
- the operator's role during and after the incident,
- interim operating instructions,
- access to off-site storage facilities,
- definitions of the user's, developer's, and vendor's roles when totally rebuilding the manual and automated systems within the facility, and
- training procedures.

The SOPs should contain detailed references to any "work arounds", or extra steps, that are necessary to perform the tasks that the computerized system does not or was not intended or designed to perform. Users should ensure that "work arounds" are included in their training program.

B. User's Manual

The vendor supplied User's Manual should contain the instructions for use of the software. It is essential that the User's Manual be written in direct, easily understandable language wherever possible. Technical jargon should be used sparingly and defined when it is used. The User's Manual should clearly define normal system operations, back-up, and restoration methods. The vendor supplied User's Manual might not contain information on disaster recovery. Therefore, the blood establishment's SOPs for disaster recovery should be clearly defined.

1. Normal System operations are tasks regularly performed by the user. Normal start-up procedures include logging on, menus and their uses, and automatic controls for user access to the functions and data [normally by password and user identification (USERID)]. Normal shut-down procedures include logging off and "house-keeping" procedures [diagnostics and archiving of data (including data back-up)] to be performed at pre-established intervals. Normal automatic functions that are performed by the computer include data edit checks, diagnostic routines, and automatic back-ups.

Normal input and output functions that are performed by the system's operators and by peripheral equipment include normal data input (e.g., keyboard entries for editing and deleting data), manipulating data that is input by peripheral equipment (e.g., test results), normal data/information output (e.g., screen displays, printed reports), and other tests to verify that the system is performing normally.

2. Back-up and Restoration Procedures should be established and followed regularly to help preserve and ensure the integrity of data. Data storage includes equipment descriptions and instructions for their use. "House-keeping" (e.g., daily, weekly, and monthly routines) include handling the physical media (e.g., mounting, labeling, and on and off site storage). SOPs should include actions to be taken when errors occur during this process [e.g., file not found, disk full, tape full, etc. (see section IX. C. Data Storage)].

C. Training Manual

Vendor supplied Training Manuals, handouts, personnel proficiency tests, and training procedures are an integral part of the system's documentation. Vendor supplied materials may help provide guidance for the training of the facility's personnel, but are not a substitute for a Training Plan in the SOPs. The user's training material should be based on the concepts, principles, and instructions found in the SOPs and the vendor supplied User's Training and Maintenance Manuals. Different training plans may be designed for use by managers, supervisors, operations personnel, and other users.

D. Maintenance Manual

Vendor provided Maintenance Manuals address the technical details of the system's structure and operation. The Maintenance Manual should provide a clear understanding of the system, including detailed system descriptions that are cross referenced with the User's and Training Manuals. Detailed descriptions of the system's hardware and software as well as their relationships within the facility should be in a user generated Maintenance Manual (including detailed descriptions of any known system and facility anomalies).

E. Document Maintenance

All SOPs and Manuals should be maintained to reflect current processes and procedures that are accomplished through the use of the computerized system.[14] The user should ensure that all SOPs and Manuals are cross referenced. Outdated SOPs and Manuals should be removed as appropriate and should be archived.[15] Proper document maintenance includes the ability to show when procedures were approved by management and implemented (i.e., effective date).

IX. MAINTENANCE

All systems require installation, validation, calibration, Quality Control (QC), and preventive maintenance, and should be included in the Quality Assurance (QA) program.[16] The user should ensure that the documentation is complete. The user has the responsibility for validation, proper use, and operation of the system.[17]

A. System Maintenance

Computerized system maintenance includes all parts of the system (e.g., hardware, software, and peripheral devices). System maintenance includes preventive and emergency maintenance as well as system evaluation audits (see Section XII. Audits). System maintenance is performed by the user in accordance with the SOPs .and vendor recommendations.

1. Preventive Maintenance tests will help to confirm that the system performs correctly and will have a minimum of downtime. All vendors should provide protocols for maintenance and tests with documentation that recommend the intervals and any calibration needs. The user should integrate this documentation and these recommendations into the SOPs to ensure that the procedures are adequate for quality control and quality assurance.

2. Utilities or diagnostic software applications help to confirm that the system is working properly and assist in ensuring data integrity. These utilities should be included in testing and validation plans, and be clearly cross referenced in the SOPs. Blood establishments should document the use of and the results obtained from these utilities.

Diagnostics are available from hardware and software vendors. Lengthy diagnostics are normally run during non-peak hours ("house-keeping") to avoid interference with normal operations.

B. Data Maintenance

The user should develop procedures that ensure that the database is kept free of unwanted duplicate and discrepant data, and to help users recognize data entry errors. Users should be advised to develop "measures" that are realistic targets to be met to satisfy that adequate quality levels have been obtained.

1. Duplicate Data may be considered to be discrepant data. System design should minimize the occurrence of duplicate data. When duplicate data occur, these data should be removed from the database as soon as possible. The user's procedures for correcting undesired or duplicate data should be clearly defined in the SOPs.

2. Discrepant Data may have serious repercussions. The database should be routinely checked as part of the system's maintenance to ensure that data are correct and properly stored. Donor identification codes should match the other donor information (e.g., the address should match the donor, the donor's deferral status should be properly identified, the test results should correspond to the correct unit ID number, and the results of all tests and repeat tests should be properly entered).

C. Data storage

Data storage and retrieval are critical parts of the system. A computer should be able to store and retrieve data accurately, on command, from both on-line and archival or back-up storage for as long as the record is required to be retained.18 On-line and archival storage (e.g., magnetic media, microfiche, optical media, paper) should be validated to ensure that the system has correctly stored (created a true and permanent copy of) the data. Validation should also ensure that data is reliably retrieved for the duration of the retention requirement and that the expected life of the storage media is sufficient to meet the retention requirement.[19]

1. On-line storage or routine storage should be handled by each system in accordance with its design. Software should contain a feature that recognizes system errors and warns the user that a problem has occurred. Some systems may not "mention" the fact that data will be lost or overwritten. The user should ensure that there is adequate protection against inadvertent data loss (e.g., when a storage device is "full" or "missing").

2. Archival Storage (long term back-up methods) should protect the user against catastrophic data loss. Archival storage uses long term storage media for data removed from the system. This storage media may be in the form of tapes, discs, or diskettes, and it should be stored off-site under appropriate storage conditions. Archival storage protocols should be clearly defined in the SOPs. The user should be cautioned to investigate lifetimes of backup media. For example it is recommended that tapes be "exercised" annually. Also, since tapes can be demagnetized with age, consideration should be given to procedures for copying data for longer storage.

X. SECURITY

All systems should have strict security controls. The security of the system and the integrity of the data should be strictly maintained. When the system or the data are changed, the changes should be clearly traceable through the use of audit trails. Systems that have connections to telephone communications through modems should have strict access controls and restrictions. Access restrictions on such systems should be designed to prevent unauthorized access or change.

Procedures that validate the hardware and software systems should rigidly test security. The use of USERIDs and passwords should be routinely tested. Validation protocols should ensure and document that sensitive donor information is not compromised, that critical data are valid, and that SOPs are correct.

A. Password and Electronic Identification

All persons authorized to have direct access to the software or data should be uniquely identified electronically. The security and access procedures selected should be strictly enforced to maintain the level of security established to ensure the integrity of the data. Records that identify system users should be maintained in accordance with requirements and recommendations. For example, the security of passwords should be ensured such that only selected persons are able to change the codes for deferred donors or quarantined units. Also, the use of both a USERID and password for electronic identification is rapidly becoming an industry standard for electronically signing a document. In state of the art computerized systems, both a USERID and password are entered for each signing from LOGON to document endorsement.

Password security includes:

- periodically changing passwords, not to be reassigned or re-used,
- deleting the access authorization for persons that no longer have a need to work with the data,
- ensuring both unique identity of individuals and their access level,
- ensuring that users use passwords that are not recognizable as reflections of their personal life (i.e., birthday, license plate number, spouse's name),
- ensuring that passwords are not shared, and
- clearly defining SOPs for personnel guidance.

B. Confidentiality

Each establishment should develop and use clearly defined SOPs to provide for the maintenance of the confidentiality of sensitive donor information. These procedures should be designed to prevent inadvertent disclosure and to guard against unauthorized external and internal inquiries.

> **NOTE: In multipurpose systems, it is strongly recommended that sensitive files be protected by password and any other means deemed necessary.**

XI. TRAINING, SUPERVISION, AND PROFICIENCY TESTING

Computer systems should be managed like all other systems in blood establishments. Training manuals provided by the hardware or software vendors should be evaluated for accuracy and incorporated into training programs as appropriate. In addition, other written training procedures relevant to the system as a whole should be prepared and used appropriately. All standard supervisory controls should be applied, including, but not limited to, routine review of all critical procedures. There should be active monitoring of employee performance and formal proficiency testing programs.

XII. AUDITS

Regular audits should be performed as a routine part of the Quality Assurance (QA) program. QA consists of the actions, planned and taken, that provide confidence that all systems and elements that influence the quality of the product are working as expected. Quality Control (QC) is a component of QA that is performed to provide assurance that at the moment the test is run the procedure is working as expected.

The blood establishment should use vendor recommendations concerning procedures to develop a QA program.[20] At a minimum, these procedures should include:

- documentation,
- system testing,
- implementation, and
- maintenance.

The user should integrate and implement the principles of quality control and quality assurance in testing and validation.[21] In the SOPs, the user should define:

- the frequency of system testing,
- the manufacturing specifications,
- the criteria for acceptability,
- the remedial action to be taken when the result of any test provides an unexpected result, and
- steps to be followed in investigating and correcting discrepancies that could lead to errors in manufacturing of blood and blood components.

A. Record Reviews

Routine reviews of the master database transaction logs, audit trail records and other logs should be performed by properly trained and authorized persons. The timing and scope of in-house record reviews should be clearly defined in the SOPs. Summaries of the review activities and corrective measures should be available to FDA Investigators upon request.

B. System QA Audits

System QA audits should be performed by specified personnel in accordance with plans that are clearly defined in the SOPs. Reviews of the computer system should be a part of each routine Quality Assurance audit. The audits of the computer system should evaluate those aspects of the system's use and performance necessary to ensure proper results. System QA audits should include, but not necessarily be limited to, review to determine that:

- all hardware and software has been subjected to all appropriate calibration, validation, and routine maintenance,
- appropriate documentation regarding the system's components is present,
- vendor upgrades, repairs, replacement of components have been evaluated for their impact on operations,
- appropriate training, supervision, and proficiency testing have been performed,
- system components are being used in accordance with applicable manufacturer's instructions, SOPs, and FDA requirements,
- procedures for change control, data maintenance, and integrity are followed, and
- problems that have been encountered with system malfunction have been appropriately evaluated and addressed.

XIII. REPORTING TO CBER

Licensed establishments must submit information describing the proposed computer system as a supplement to the Establishment License Application (ELA).[22] Requests for supplement approval should contain the following information:

1. Identification of the hardware, including the central and peripheral devices and network linkages.

2. Identification of the source(s) of the application software used, this should include the name of the software vendor, the name and version number of the software package.

3. The location(s) where computer(s) will be used. Include donor collection centers, self-contained mobiles, and the distribution centers.

4. A brief description of how the computer system will be used and in what areas of the facility.

An important proposed change to a computerized system is also reportable as a supplement to an ELA.[23] This includes any hardware or software modification or enhancement that may affect the way that the data are manipulated or interpreted prompting a revalidation of the computerized system (e.g., calculations for a decision making process such as donor suitability or unit release).

Supplements to the ELA should be sent to:

Food and Drug Administration
Center for Biologics Evaluation and Research
Document Control Center (HFM-99), Suite 200N
1401 Rockville Pike
Rockville, MD 20852-1448
Attn: Division of Blood Establishment and Product Applications, (HFM-370)

XIV. REFERENCES

A. **Title 21, Code of Federal Regulations**

A listing of the sections of Title 21, Code of Federal Regulations (21 CFR) that are related to computerized systems include:

1. **21 CFR, Part 200** - Drugs: General

2. **21 CFR, Part 210** - Current good manufacturing practice in manufacturing, processing, packing, or holding of drugs; general

3. **21 CFR, Part 211** - Current good manufacturing practice for finished pharmaceuticals

4. **21 CFR, Part 600** - Biological products: General

5. **21 CFR, Part 606** - Current good manufacturing practice for blood an blood components

6. **21 CFR, Part 610** - General biological products standards

7. **21 CFR, Part 640** - Additional standards for human blood and blood products

8. **21 CFR, Part 800** - Medical Devices: General

9. **21 CFR, Part 820** - Good manufacturing practice for medical devices: general

B. Food and Drug Administration Publications

The FDA documents that deal with computers and compliance issues, including reference materials and training aids for investigators, are:

Blood Bank Inspection Checklist and Report and accompanying instructions.

Form FDA 2609 (5/91), Section K, Computerization, contains questions that are asked by the Investigators during an inspection.

Guide to Inspection of Computerized Systems in Drug Processing

February, 1983. FDA, Division of Drug Quality Compliance and Division of Field Investigations. U.S. Government Printing Office 1983-381-166:2001

Technical Report on Software Development Activities

July, 1987. FDA, Office of Regulatory Affairs

Guideline on General Principles of Process Validation

May, 1987. FDA, Center for Drugs and Biologics and the Center for Devices and Radiological Health

Reviewer Guidance for Computer Controlled Medical Devices Undergoinq 510(k) Review

August, 1991. FDA, Center for Devices and Radiological Health

Draft Guideline for Quality Assurance in Blood Establishment

Docket No. 91N-0450, June 17, 1993. FDA, Center for Biologics Evaluation and Research

C. Memoranda

Food and Drug Administration memoranda issued by the Center for Biologics Evaluation and Research (CBER) to All Registered Blood Establishments[24]:

Subject: Responsibilities of Blood Establishments Related to Errors & Accidents in the Manufacture of Blood & Blood Components
Date: March 20, 1991

Subject: Deficiencies Relating to the Manufacture of Blood and Blood Components
Date: March 20, 1991

Subject: Requirements for Computerization of Blood Establishments
Date: September 8, 1989

Subject: Recommendations for Implementation of Computerization in Blood Establishments
Date: April 6, 1988

XV. GLOSSARY

ARCHIVE an indelible collection of computer system data or other records that are in long term storage. Backing-up the database is the first step in creating a computer generated archive. The steps in creating and safely maintaining an archive should be clearly defined in the SOPs.

CHANGE CONTROL the processes, authorities for, and procedures to be used for all changes that are made to the computerized system and/or the system's data. Change control is a vital subset of the Quality Assurance (QA) program within an establishment and should be clearly described in the establishment's SOPs.

COMPUTER SYSTEM an electronic device controlled by lists of instructions (programs). The computer system is used by its operators (personnel) to perform specific tasks. The "system" includes the resources used to complete a task (i.e., computer system [hardware, software], personnel, peripheral equipment [e.g., test equipment, printers, disk drives]). Validation confirms that the system is functioning according to specifications.

CONFIDENTIALITY OF DONOR INFORMATION broadly covers any means by which the unauthorized disclosure of sensitive data or information is prevented. Sensitive data are the personal details about the donor (i.e., test results, deferral status).

DATABASE (1) A set of data or part of a set of data consisting of at least one file that is sufficient for a given purpose or for a given data processing system. (2) A collection of data basic to a system. (3) A collection of data basic to an enterprise.

DATABASE SECURITY means by which the confidentiality and integrity of a database is maintained.

DEVELOPER a person, or group, that designs and/or builds and/or documents the hardware and/or software of computerized systems.

DEVELOPMENT METHODOLOGY a systematic approach to software creation that defines development phases and specifies the activities, products, verification procedures, and completion criteria for each phase.

DISASTER PLAN the part of an establishment's SOPs that contains detailed instructions on what to do in the event of a catastrophe. The disaster plan is an <u>essential</u> part of the establishment's SOPs.

DOCUMENTATION (1) A collection of documents on a given subject. (2) The management of documents, including the actions of identifying, acquiring, processing, storing and disseminating. (3} Any written or pictorial information describing, defining, specifying, reporting or certifying activities, requirements, procedures, or results. NOTE: As an indelible record, documentation is an indispensable tool of validation.

FIELD discrete location in a database that contains an unique piece of information. A field is a component of a record. A record is a component of a database.

FLOW CHART the graphical representation of the logical steps involved in a procedure or program. A flow chart is a part of the documentation of the structure of a computer program or system. Flow charts may be included in the Program Maintenance Manual.

HARDWARE the physical equipment that is part of the computer system (e.g., chassis, keyboard, monitor).

INSTALLATION includes installing a new computer system, new software or hardware, or otherwise modifying the current system.

LEVEL OF SECURITY determines what functions a user is authorized to perform. Authorization is determined by the level of security assigned to the USERID and password. The basic levels of security are READ and WRITE. There are many variations and combinations of security that can be achieved by limiting the user's ability to VIEW certain data. For example, a user could be permitted to READ a donor's address and deferral status but only WRITE or change the donor's address. Levels of security and access to the functions of the system are strictly controlled by the System Administrator.

MODEM an electronic device used to communicate between two or more computers using a communications protocol.

MODEM ACCESS using a MODEM to communicate between computers. MODEM access is often used between a remotely located computer and a computer that has a master database and applications software.

MULTIPURPOSE SYSTEMS computer systems that perform more than one primary function or task are considered to be multipurpose. In some situations the computer may be linked or networked with other computers that are used for administrative functions (e.g., accounting, word processing).

OPERATING SYSTEM software that controls the execution of programs, including such services as resource allocation and scheduling, input/output control, and data management. Although operating systems are predominately software, partial or complete hardware implementations are possible.

ORIGINAL EQUIPMENT MANUFACTURER (OEM) person or company that originally built a component part or system.

PASSWORD an alphanumeric word (string of characters) that is unique to each USERID. A password is used when logging on to a computer system. A password is used with a USERID to determine the levels of access that will be granted to a user.

PERIPHERAL DEVICE equipment that is connected to the Central Processing Unit (CPU). A peripheral device can be used to input data (e.g., laboratory test equipment) or to output data (e.g., printer, disk drive, video system, tape drive).

PRODUCTION DATABASE the computer file that contains the establishment's current production data.

RECORD OF CHANGE documentation of changes made to the system. A record of change can be a written document or a database. Normally there are two associated -with a computer system (hardware and software). Changes made to the data are recorded in an audit trail.

REGION a clearly described area within the computer's storage that is logically and/or physically distinct from other regions. Regions are used to separate testing from production (normal use).

SEARCH and RETRIEVAL ALGORITHMS procedures that a computer uses to locate data within a database.

SITE SURVEY conducted to determine the characteristics of the site in which a system is to be installed. These surveys include the location, stability and availability of utilities (including air conditioning), and the physical layout of the site (including access to rooms and hallways).

SOFTWARE computer programs, procedures, rules, and associated documentation and data pertaining to the operation of a computer system.

SOURCE CODE human readable version of the list of instructions (program) that cause a computer to perform a task. A computer program that must be compiled, assembled, or interpreted before being executed by a computer.

SYSTEM ADMINISTRATOR the person that is charged by the Responsible Head with the overall design, administration, and operation of the organization's computerized systems. The System Administrator is normally an employee or a member of the establishment.

SYSTEM DEVELOPER may be the user, a contracter, a vender, or a software device manufacturer. See also developer.

SYSTEM DEVELOPMENT METHODOLOGY (SDH) or Life Cycle Methodology is a structured method used to plan, design, validate, and implement a system.

SYSTEM DOCUMENTATION the documentation of the requirements, design philosophy, design details, capabilities, limitations, and other characteristics of a system.

TEST DATABASE contains a mix of production and test data. Test data will have deliberately introduced errors. A test database is kept and used in a region (partition) that is segregated from the production software and database to prevent serious problems.

USER An individual or organization that normally supplies information for processing, or that receives, interprets, and uses the output or effects of such processing.

USERID an alphanumeric word (string of characters) that is unique to each user. The USERID is used when logging on to a ,; computer system. The USERID is the primary key that it determines the level of access that will be granted to the user.

VALIDATION the establishment of documented evidence (for example, data derived from rigorous testing) which provides a high degree of assurance that a specific process or system will consistently produce a product meeting its predetermined specifications and quality attributes.

VENDOR person or organization that provides, as a medical device manufacturer, software and/or hardware and/or firmware and/or documentation to the user for a fee or in exchange for services.

XVI. ENDNOTES

1. See, e.g., 21 CFR 211.68, 211.100, 211.180, 211.188, 211.194, 600.10(a) and (b), 600.12(a) and (b), 606.20(a) and (b), 606.60, 606.100, 606.160.

2. See, 21 CFR 601.12(a).

3. See, e.g., 21 CFR 600.10(a) and (b), 606.20(a) and (b), 606.60, 606.100, 606.160, 211.63, 211.67, 211.68, 211.100.

4. See, e.g., 21 CFR 600.10(a) and (b), 606.20(a) and (b), 606.100, 606.160, 211.63, 211.67, 211.68, 211.100, 211.180.

5. See, e.g., 21 CFR 600.10(a) and (b), 606.20(a) and (b), 606.100, 606.160, 211.63, 211.67, 211.68, 211.100, 211.180.

6. See, e.g., 21 CFR 606.160, 211.68(b), 211.194.

7. See, 21 CFR 211.100, 211.110(a), 606.100.

8. See, e.g., 21 CFR 211.68, 211.110, 211.100(a) and (b), 606.160(b)(5)(i) and (ii), and Guideline on General Principles of Process Validation.

9. See, 21 CFR 606.60 (a) and (b).

10. See, e.g., 21 CFR 211.63, 211.68.

11. See, e.g., 21 CFR 211.22(c), 211.68, 211.100(a).

12. See, e.g., 21 CFR 211.68(a), 606.160(b)(5)(i) and (ii).

13. See, e.g., 21 CFR 606.100, 211.100.

14. See, e.g., 21 CFR 606.100, 211.100(a).

15. See, 21 CFR 606.100.

16. See, e.g., 21 CFR 606.60, 606.140(b), 211.100, 211.110(a), 211.68(a).

17. See, e.g., 21 CFR 600.10(a).

18. See, 21 CFR 606.160(d), 211.180(a) and (b), 211.198.

19. See, e.g., 21 CFR 211.68(b).

20. See, Center for Biologics Evaluation and Research (CBER), Draft Guideline for Quality Assurance in Blood Establishments, Docket No. 91N-0450, June 17, 1993.

21. See, 21 CFR 211.22.

22. See, 21 CFR 601.12(a).

23. See, 21 CFR 601.12(a).

24. Copies of the Food and Drug Administration Memoranda issued by CBER to All Registered Blood Establishments are available through the Division of Congressional and Public Affairs, 1401 Rockville Pike Suite 200N, Rockville, MD 20852-1448. FAX (301) 594-1938. There may be a charge in accordance with Department of Health and Human Services regulations.