APPLICATION OF THE MEDICAL DEVICE GMPS TO COMPUTERIZED DEVICES AND MANUFACTURING PROCESSES

MEDICAL DEVICE GMP GUIDANCE FOR FDA INVESTIGATORS

Prepared by
Office of Compliance and Surveillance
Division of Compliance Programs

November 1990

FIRST DRAFT

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Public Health Service
Food and Drug Administration
Center for Devices and Radiological Health
Rockville, Maryland 20850

CONTENTS

SECTION		PAGE
1.0	PURPOSE	1
2.0	SCOPE	1
3.0	INTRODUCTION	1
4.0	APPLICATION OF THE GMP REGULATION	1
4.1	General	1
4.2	Organization & Personnel (820.20)	2
4.2.1	Quality Assurance Program Requirements (820.20(a))	2
4.3	Personnel Training (820.25(a))	5
4.4	Environmental Control (820.46)	6
4.5	Equipment (820.60)	7
4.6	Measurement Equipment (820.61)	8
4.7	Components (820.80)	9
4.7.1	Acceptance of Components (820.80(a))	9
4.7.2	Storage & Handling of Components (820.80(b))	10
4.8	Critical Devices, Components (820.81)	11
4.9	Manufacturing Specifications & Processes (820.100)	12
4.9.1	Processing Controls (820.100(b))	14
4.10	Finished Device Inspection (820.160)	14
4.11	Failure Investigation (820.162)	15
4.12	Records, General Requirements (820.180)	16
4.13	Device Master Record (820.181)	16
4.13.1	Specifications (820.181(a))	16
4.13.2	Production Process Procedures (820.181(b))	17
4.13.3	Quality Assurance Procedures & Specs. (820.181(c))	18
4.13.4	Labeling (820.181(d))	18
4.14	Device History Record (820.184)	18
4.15	Critical Devices, Automated Data Processing (820.195)	19
4.16	Complaint Files (820.198)	19
APPENDIX A -	DEFINITIONS	21
APPENDIX B -	REFERENCES	23

Application of Medical Device GMPs to Computerized Devices and Manufacturing Processes

1.0 PURPOSE

This document outlines GMP requirements as applied to the manufacture of computerized devices and the control of computerized manufacturing and quality assurance systems. It is intended to provide guidance to FDA investigators and to supplement FDA document 84-4191, Medical Device GMP Guidance for FDA Investigators.[1] This document is also designed to supplement FDA issued compliance policy statements and references on Software Development Activities Policy Guides[2] and FDA's Technical Reference on Software Development Activities.[3]

2.0 SCOPE

This document applies to manufacturers who utilize automated systems for manufacturing, quality assurance, and/or recordkeeping. It also applies to manufacturers of medical devices that are driven or controlled by software.

3.0 INTRODUCTION

The GMP contains requirements which assure that specifications are established for the device, components, labeling, and packaging and that these specifications are met. The GMP is written in general terms in order that it may apply to a broad diversity of medical devices and manufacturing processes found in the medical device industry. Because of this, FDA investigators sometimes have difficulty in applying the GMP to certain aspects of the industry. Automation is one area where investigators have expressed difficulty in applying the GMP, whether it is automation of individual devices or automation of a manufacturing system.

This document is intended to assist investigators in properly interpreting and applying the GMP to this industry. However, investigators should understand that while the procedures and controls described in this document are acceptable to FDA, they may not be the only procedures and controls acceptable to FDA. Manufacturers are free to use other approaches as long as they can provide assurance that they are adequate in meeting the applicable GMP requirements.

4.0 APPLICATION OF THE GMP

4.1 General

In order to assure that only safe and effective devices are distributed, devices must be designed and manufactured under adequate quality assurance controls. The following is a section-by-section discussion of the GMP as it applies to computers and describes the types of controls that would

typically be expected. The actual controls utilized by a manufacturer may differ from those described. When they do, investigators should obtain justification from the manufacturer.

The validity of the manufacturer's approach should be evaluated in terms of the manufacturer's demonstrated degree of success in applying the approach to the manufacture and distribution of only safe and effective devices.

4.2 Organization (820.20)

The GMPs require all manufacturers of medical devices to establish and implement an organizational structure that includes a formal quality assurance program and sufficient personnel to assure that all devices are manufactured in accordance with the GMPs. The program that a manufacturer establishes to implement the GMP requirements effectively becomes the firm's quality assurance program.

In order to comply with the GMP requirements, manufacturers organize themselves in such a way that there is adequate and continuous control over all activities affecting quality. Technical, administrative and human factors affecting quality of the products produced are properly controlled. Such controls are oriented towards the reduction, elimination and prevention of quality deficiencies.

The responsibility, authority and the interrelation of all personnel who manage, perform and verify work affecting quality is defined. The program emphasizes the identification of actual or potential quality problems and the initiation of remedial or preventive measures.

All the elements, requirements and provisions adopted by a company for its quality assurance program are documented in a systematic and orderly manner in the form of written policies and procedures. Such documentation (e.g. quality plans, manuals, records, etc.) ensures a common understanding of quality policies and procedures.

Management assigns an individual the responsibility and authority for ensuring that the requirements of the GMP are implemented and maintained.

Part 820.20(a) contains some specific responsibilities of the QA program.

4.2.1 Quality Assurance Program Requirements (820.20(a))

Part 820.20(a)(1) of the GMP mandates that all production records must be reviewed. This requirement applies equally to manual and computerized records.

Per Part 820.20(a)(2) each manufacturer is responsible for assuring the acceptability of components and labeling, as well as the finished device, regardless of whether they are manufactured in-house or provided under contract by another company (vendor supplied). Therefore, a manufacturer's quality assurance program includes procedures for assuring approval or rejection of contract-supplied software.

To assure that only acceptable software is received, manufacturers who purchase software from vendors establish a program for assuring that the vendor has demonstrated a capability to produce quality software. The program provides assurance that the requirements for the software are clearly defined, communicated and completely understood by the vendor. This may require written procedures for the preparation of requirements and purchase orders, vendor conferences prior to contract release and other appropriate methods. In order to assure understanding, manufacturers establish a close working relationship and feedback system with the vendor. In this way a program of continual quality improvements can be maintained and quality disputes avoided or settled quickly.

Acceptance procedures for contract-supplied software may vary. For example, they may include third-party certification. The finished device manufacturer, however, has the primary responsibility for assuring the software is adequate for its intended use. When third-party certification is used, the certification package includes adequate documented evidence that the software complies with specified requirements. Examples of such evidence include documentation of the review, including procedures used to evaluate the software, the results of the evaluation and evidence of the decision-making process used by the manufacturer to conclude that the software will fulfill its requirements. When the contract-supplied software includes more functions than are utilized, those portions of the program which will be used are evaluated for their application. Also, the software is evaluated to assure the unused portions do not interfere with proper performance. Specific requirements which apply to these activities are covered under 820.80(a), 820.160, and 820.161 and are discussed later in this document.

Part 820.20(a)(3) requires manufacturers to identify quality assurance problems and to verify the implementation of solutions to those problems. Thus, quality data collected by a firm through its various documented process and control systems, such as work operations, processes, quality records, service reports and customer complaints, are evaluated by appropriate methods (e.g.,

trend analysis) to determine if there are trends or recurring problems which warrant corrective action.

These reviews are an important element of an effective quality assurance program and are important for identifying conditions or situations (e.g., device design problems or problems associated with the manufacturing process) which might not otherwise be apparent or might be dismissed as isolated incidents. The results of investigations and corrective actions are, of course, documented.

Per 820.20(a)(4) all quality assurance checks must be appropriate and adequate for their purpose and must be performed correctly. QA software checks may be both quantitative or qualitative; testing is not restricted to quantitative measurements. Testing of software involves evaluation of conformance to specifications and ability to perform as intended. Therefore, test results may vary in expression from a numerical value which is the checksum for the program or the result of a complex mathematical calculation to a qualitative determination, such as the functional adequacy of the illumination of a light or a display.

QA checks of the original program before it is released to manufacturing include review of documentation to assure that the program conforms to its design specifications, which are covered by 820.181(a), as well as an evaluation to assure it performs as intended. It is common for the program to be evaluated as segments or modules first, then as an integrated unit, and finally a system. The documented test results are evidence of the evaluation. When software is involved in manufacturing and quality assurance, evaluation is covered by 820.100(a)(1) and 820.61. This evaluation is performed when software is developed in-house, and, when it has been supplied by a vendor.

After the program has been accepted, and released to production, it is evaluated to assure that it is accurately transferred/copied from storage medium to storage medium (e.g., magnetic disks to integrated electronic circuitry chips). The evaluation also assures that the working master copy remains an exact duplicate of the program that was approved and released to production and that the software has not undergone unapproved revision or modification.

Section 820.20(b) requires manufacturers to conduct planned and periodic audits of their quality assurance program. Every quality audit includes a review of procedures and activities to assure standard operating

procedures are adequate and are being followed and that all elements of the quality system are effective in achieving stated quality objectives. As applied to software, this audit includes evaluation of procedures used to assure that hardware and software are adequate for their intended use, and that SOPs remain adequate. The audits extend to all phases of software design, development, testing, design transfer, implementation, and maintenance activities related to computerized processes and devices.

Since in many cases manufacturers rely on suppliers to assure quality of software, the quality audit includes the supplier. On-site assessments are made of the supplier's capability to produce quality software and other components.

Audits are conducted by individuals qualified to perform the task. Evidence is available to show that individuals involved in software QA review and evaluation have been adequately trained. As with any other device manufacturing process, these individuals have a working knowledge of how the device is made, and they should also have a working knowledge of developing and documenting software.

The results of the audits are documented and brought to the attention of the personnel responsible for the areas audited and upper management. Timely corrective action is carried out and verified as necessary.

4.3 Personnel Training (820.25(a))

All personnel must have adequate training to perform their assigned responsibilities. This means that individuals responsible for producing and evaluating software have the necessary education, training, and experience to assure that the software is properly prepared and maintained. These individuals know how to develop the software and have an understanding of how to properly document and test the program to minimize, with an adequate degree of confidence, the effect of latent faults.

Also of concern are the training, experience, and knowledge of employees responsible for duplicating software and handling magnetic storage media (e.g., floppy disks, tapes, PROM chips, etc.). Training is conducted to assure these individuals are fully aware of their responsibilities, particularly of the controls and procedures they must follow to assure that software incorporated into the final medical device is not adversely effected and performs as intended. Appropriate records of training/experience are maintained.

4.4 Environmental Control (820.46)

Where environmental conditions could have an adverse impact on a device's fitness for use, the conditions must be controlled. In general, this applies to the manufacturing environment and areas used for storage of components, and the finished device.

Computers and software storage media may be sensitive to the environment. Mainframe (and some mini-) computers generally call for stringent temperature and humidity controls, and all computers are subject to some degree of environmental limitations.

Overheating, whether from an external source or from the computer's own electronic circuits, can have an adverse effect on a computer's ability to operate properly. Failures caused by system overheating may range from total failure or shutdown of the system to intermittent errors. The maximum temperature at which a microprocessor or central processing unit (CPU) can operate is usually stated in the processor/CPU specifications established by the system's manufacturer.

Humidity may also adversely affect a computer system. Because the computer system is an electronic unit, excessive humidity can have a detrimental effect on electrical contacts and circuitry within the system. Conversely, a dry environment will increase the possibility of static discharges that can damage electrical circuits, software storage components (e.g., chips, and other static sensitive components) and, in turn, have an adverse effect on the software.

The degree of environmental control required is determined by the manufacturer of the finished device. Specifications are developed for the environment and maintained in the device master record. A control system is implemented to assure that the environmental specifications are not exceeded. This environmental control system is periodically inspected for proper functioning and the inspections are documented.

Some electronic hardware components such as computer chips which house the software assembled in the device, are sensitive to electrostatic discharge (ESD). When ESD is a concern, only personnel at properly ESD-controlled work stations handle blank static-sensitive chips, preprogrammed chips, and the circuit boards containing these chips. ESD controls include grounding, humidity control, negative ion generation, etc. The firm's system for controlling ESD is periodically inspected to assure it is exercising adequate control: Are work stations properly grounded? Are employees, working with ESD-sensitive components grounded to work stations? Is humidity monitored? Routine inspections are part of the equipment maintenance procedures.

Other forms of preprogrammed media such as disks (hard and floppy) and magnetic tapes are also handled only in environmentally controlled areas. In areas where these are used, the ability to retrieve data may also be adversely affected by exposure to dust and dirt; therefore, dust and dirt is controlled in addition to ESD.

Components and other media are protected from sources of magnetic interference which can result in the potential accidental erasure of the software by a magnetic field from a permanent magnet or electromagnet. If the product is electromagnetic interference (EMI) sensitive, then efforts to control and/or test for EMI are documented.

4.5 Equipment (820.60)

Section 820.60 of the GMP mandates periodic maintenance of equipment used in the manufacturing process, when applicable. When applied to the software used in production, working master copies of software are periodically challenged and compared against the archived master as a means of assuring that the working copy of the released version is a true copy of the master. Unauthorized changes may compromise the accuracy and reliability of the process.

Comparison of two or more computer programs may be accomplished by a number of different procedures. One common method uses a software utility program which compares two programs and prints differences found between them. A comparison of disk directories between the master and working copies as well as the use of some comparative programs can assist in identifying the differences. The differences may be as simple as one copy containing additional utility programs while the others do not. Another procedure involves comparing the checksums of the preprogrammed chips. The checksum is the value which results from the addition of the values stored in each address on the chip. The values from each chip of the working copy are then compared with the checksums of the archived master. Any difference between the two reflects a discrepancy in the programs and indicates a change in either of the two copies, but it does not identify the location of the difference(s). This is accomplished separately.

Only the current version of software that has been approved and released for use by the device manufacturer is available in the manufacturing/quality control area. When software revisions have been made and released for use, obsolete versions of the program are removed from use. Appropriate corresponding documentation (e.g., written manufacturing procedures and/or design specifications) is also updated and distributed in a timely manner.

A written maintenance procedure is recommended as a dependable means for assuring that all aspects of equipment maintenance are covered.

4.6 Measurement Equipment (820.61)

All computerized production and quality assurance measurement equipment must be suitable for its intended use and capable of producing valid results. To establish confidence in the adequacy of computerized equipment, the hardware (sensors, transmitters, etc.) is calibrated and the software is challenged and validated to assure fitness for its intended use. Calibration is done in accordance with written calibration procedures and schedules. The frequency of calibration may be dependent upon the purpose of the measurement taken, stability, and how often the equipment is used.

Calibration of computer hardware is similar to calibration of any other electromechanical system. The sensor's measurement of temperature, voltage, resistance, etc., is compared against the measurement of a known standard traceable to the National Institute of Standards and Technology (formally the National Bureau of Standards) or other acceptable standard. An important part of the calibration activity is to assure that measurements are properly transmitted across computer communication lines and properly interpreted by the computer system.

Verification of properly transmitted measurements is accomplished by comparing the measured value that has been input into the computer system with the value of the traceable standard.

The PROM programmer, a piece of manufacturing equipment, is used for programming integrated circuits (ICs). To assure that integrated circuits are adequately programmed, equipment maintenance and calibration needs for programmers should be considered, including proper voltage, current, and pulse shape.

Modification of the hardware and/or configuration of the system may require system recalibration. Procedures for handling modifications are addressed in standard operating procedures.

When automated production or QA systems are used, the software programs are validated. Validation of system software is a complex activity which must be carefully planned and performed, before use of the software package, and after significant revision of the system occurs. Validation may also be required after any revision of the operating system software. Software verification and validation activities are discussed in greater detail in FDA's reference manual, Software Development Activities.[2]

4.7 Components (820.80)

The GMP regulation requires that manufacturers establish adequate procedures for acceptance and storage of components to assure that only those components that are acceptable for use are released to manufacturing.

4.7.1 Acceptance of Components (820.80(a))

The components of a software driven device typically consist of circuit boards, resistors, transistors, and other discrete items commonly found in electrical devices. However, there are two additional components of special concern in a software driven device: the actual software that controls functions of the device and the hardware on which the software is stored or mounted.

Software inspection and testing are normally accomplished in a manner different from that performed on the discrete components of the device. The component specifications for software are usually referred to as the software requirements. These include user or device requirements (e.g., the device will respond in a specific manner to a specific input), and they also cover system requirements which are functions associated with the internal workings of, or handling of, data by the software. System requirements may include functions such as error checking, polling, fault tolerance, etc. Ability of the software to meet both user and system requirements is crucial to proper operation of the device.

Preparation and use of an adequate test plan, based on knowledge of software logic and the hardware environment in which the software will run, will assure that software is adequately tested or evaluated, and thereby establish confidence that it does meet specifications. In most cases, evaluation of the software requires not only testing separately from the device by simulation testing (which may use a database with known inputs) but also by testing it in the environment in which it will be used (i.e., the finished device). For example, a database which includes signals of ventricular fibrillation may be used to evaluate one function of a cardiac monitor. Because of the complexity of both software and hardware, this testing may be performed as part of the manufacturer's software development and software quality assurance activities. These tests are routinely referenced as software verification and validation. Final versions of approved test procedures constitute written component acceptance procedures for the software and results of the final tests document that acceptance criteria have been met.

After it is determined that the software is acceptable for use, consideration is given to the need for periodic retests. Retests are usually necessary when the software (operating system or application program) is revised or a software failure is encountered.

When preprogrammed storage media such as chips, disks, etc., are received as components, acceptance procedures assure that software contained in these components is the current version and that it has been adequately duplicated. Acceptance evaluation can be accomplished in a number of ways. One method is a bit-by-bit comparison of the software program in the incoming component against a known correct master copy of the program. Another method consists of determining the checksum of the software in the incoming component and comparing it against the known checksum for the current version of the program. (This test method has been previously discussed in the "Equipment" section of this document; however, the method is also applicable to acceptance of components.) These tests only assure accuracy of the reproduction efforts; they do not reflect the quality of the software program, which can only be determined through the verification and validation test efforts previously discussed.

Incoming acceptance procedures for unprogrammed (blank) ICs vary. They may consist of electrical tests or only a visual examination, depending upon whether history has demonstrated that the supplier can consistently provide a quality product.

Some medical device manufacturers may purchase OEM (Original Equipment Manufacture) products such as CRTs, computers, etc., and combine these products into a medical device system. These may be considered components rather than finished devices. In such cases, it is the medical device manufacturer's responsibility to assure the OEM products are acceptable for use. This may include testing the products individually and as part of the finished system to assure they conform to specifications.

4.7.2 Storage and Handling of Components (820.80(b))

As with all finished device components, software must be adequately identified to prevent mix-up and adequately stored to prevent damage.

Software contained on media such as disks, etc., is identified by providing name or title and version or revision level of the software. This serves to prevent use of obsolete versions of the program.

Programmed media can be damaged by the environment. For example, it is possible that software may be accidentally altered if the hardware which contains the software program is exposed to electrostatic discharge (ESD), or to ultraviolet radiation. Therefore, manufacturers exercise care in the handling and storage of magnetic media and programmed chips. (ESD control has already been covered in this document under 4.4 Environmental Control (820.46)).

Employees engaged in handling ESD sensitive components are properly trained and made aware of the results of improper performance or poor ESD control practices.

Electrostatic sensitive chips are stored in ESD protective carriers before they are assembled into circuit boards. Under some conditions, materials promoted for ESD control can actually contribute to ESD. Therefore, materials used are qualified for their use to assure adequacy. Circuit boards containing these components are also protected against ESD damage. It is also important that preprogrammed chips and circuit boards that contain preprogrammed chips be handled only by properly trained personnel at properly ESD controlled work stations.

Some hardware components, whose software can be erased by ultraviolet light, require a protective covering over the erasing "window" of the component. If the window is left uncovered, the program contained on the component may possibly "fade" in time through exposure to fluorescent light, sunlight, or other sources of UV radiation. Protective covers may include a special plastic cap or a piece of light resistant tape placed over the window.

As previously described under 4.4 Environmental Control (820.46), exposure to dust or dirt may affect the ability of preprogrammed magnetic media, such as disks or tape, to record and read data. Contents of the disk or tape may also be altered if stored in the vicinity of a strong magnetic field. Therefore, these media are protected from rough handling and temperature extremes, as well as magnetic fields and electromagnetic radiation.

4.8 Critical Devices, Components (820.81)

In addition to the requirements of 820.80 as described above, additional controls are established and implemented for handling critical components of a critical device. Section 820.81(a) requires that specific controls be in place for the acceptance of critical components. Computer components such as integrated circuits (ICs) may be identified as critical components when they are used in a critical device. The complexity of these components can make it difficult for the device manufacturer to

adequately test these components for acceptance. In this situation, the device manufacturer may have to rely on the component manufacturer to certify in writing that the required specifications have been met, and require the component manufacturer to provide actual test data. A vendor QA program (as discussed on page 3) is also established to assure confidence in the data.

GMP section 820.81(b) requires that, where possible, the finished device manufacturer must obtain a written agreement from the supplier of critical components which states that the device manufacturer will be notified of any proposed change in a critical component. In relation to computerized devices, this section applies to both hardware and software components that are critical. Hardware may include custom designed components such as gate arrays, programmable logic arrays, ROMs, and analog arrays which may have been made specifically to the finished device manufacturer's specifications. Critical component software may include programs which perform and control critical functions of a device. Whether the components are customized hardware or are a software program, it is important that the finished device manufacturer know when the component supplier makes any changes because a change to a component may adversely impact the finished device.

4.9 Manufacturing Specifications and Processes (820.100)

Specifications and procedures for manufacturing a device must be established, implemented and controlled to assure that the device conforms to its original design or to any approved changes in that design (820.100).

Section 820.100(a)(1) requires all manufacturers to assure that design requirements are properly translated into device and component specifications which are used in production. When applied to computerized operations, this means that manufacturers are prepared to provide evidence that the software used for duplicating the device software and the software used in automated manufacturing or quality assurance meets the software design specifications.

This section is interpreted by FDA to include process validation. When a manufacturing process is automated, the computerized system is validated to assure it performs as intended. In validating computerized equipment, parameters that the system is designed to measure, record, and/or control are evaluated by an independent method until it is demonstrated that the computer system will function properly in its intended environment.

When a manufacturing process is controlled by computer, functional evaluation of the control system may include, but is not limited to, the following activities:

- o equipment (peripherals, etc.) and sensor checks using known inputs, which may consist of processing test or simulated data;
- o alarm checks at, within, and beyond their operational limits; and,
- o evaluation of operator override mechanisms for how they are used by operators and how they are documented.

In case of system failure, evaluations would include:

- o how data is updated when in manual operation;
- o what happens to data "in process" when the system shuts down;
- o what procedures are in place to handle system shutdown; and,
- o how product or information handled by the computerized process is affected.

Process validation is conducted to evaluate the effectiveness and repeatability of the process and its impact on the device during both expected operation and worst case situations. When software is involved, this activity may in many cases have to be accomplished in two steps: first, the software is integrated into the system and the system is evaluated independently of the system it is to control; second, the software is integrated into the system and the system is evaluated.

Section 820.100(a)(2) requires that changes to specifications of a device, which includes software specifications, must be subject to controls as stringent as those applied to the original software program. Usually, this means validation that includes an evaluation of how the change impacts on the rest of the software. For example, if the addition of a subroutine or function is determined to have little effect on the device or process, only a limited number of modules may require retesting and revalidation. On the other hand, changes such as updating the operating system software could have an impact on the entire application software, thereby requiring more intensive evaluation. In any event, all changes are evaluated to assure that they are appropriate (that they achieve their intended purpose) and that they do not adversely affect the unchanged software.

Revisions to software follow established change control procedures to assure that the history of the changes are

maintained and that each change is properly reviewed, approved and dated before implementation.

In order to control and maintain the software and to know its configuration at any time, documented evidence is needed to demonstrate why each change was made, that each change is adequate, and that it has been approved for use. As with any device, this information is essential for investigating device defects.

Also, if the change significantly extends the indication for use, or affects the safety or effectiveness of the device, a new 510(k) or PMA supplement may need to be submitted to FDA. If the change is made to correct a problem with respect to safety, effectiveness or performance, a recall may be needed.

4.9.1 Processing Controls (820.100(b))

When the possibility exists for the device to deviate from its design specifications as a result of an inadequately controlled manufacturing process, written manufacturing procedures must be established. As applied to software, this GMP provision includes the process of duplicating the currently released, approved "master" software program onto other storage media, generally for assembly into the device. To assure that this process is adequate and produces consistent results, manufacturers have established written procedures.

Standard operating procedures (SOPs) for software handling and duplication are controlled documents. Any changes or revisions made in these documents are subjected to formal review and approval by designated individual(s) before implementation. Once approved, the revised procedures are conveyed to appropriate personnel in a timely manner.

Process controls also include computer security and may involve limiting physical access to the computer on which the software is written and/or tested and also may include limiting access to the software itself to prevent unauthorized changes. Software security may include the use of passwords, passkeys, etc. Assignment and use of these security measures should also be controlled.

4.10 Finished Device Inspection (820.160)

Adequate procedures must be in place and implemented to assure that the finished device meets its design specifications. Testing should verify that the software functions utilized perform as intended and that unused functions do not adversely affect performance. For software driven devices, it is

sometimes impossible to fully qualify the computer program through performance of function tests. Because of the computer program's logic and branching capabilities, a specific task performed by the device may be accomplished in one manner, one time, and depending on the logic of the program and the data entered, in a totally different manner another time. Therefore, independent testing of the software itself is conducted if the true capabilities and limitations of the device and software are to be known. This was discussed earlier in the "Components" section of this document. Rarely can the full functional capabilities of the software be demonstrated by testing only the finished device.

Therefore, once the software has been accepted as a component for use, and adequate control of the duplication process during manufacturing has been established through validation and process control, it is usually not necessary to re-verify performance of software in each unit, batch, or lot of devices manufactured. Instead, assurance is established that the correct version of the software program is included with the device. One way to do this is to access the program and call up its current revision or version identification either on a visual display or a printout. This method, however, is not always possible. A second method consists of verifying that the labels on the program chips or magnetic media reflect the proper software revision level identified in the device master record (DMR).

Finished product inspection of a software driven medical device also includes tests normally associated with an electromechanical device. Although these tests may not fully challenge the software, they help to assure that the device has been properly assembled.

4.11 Failure Investigation (820.162)

When failure occurs in a distributed software driven device or in a distributed device which consists solely of software, an adequate investigation must be conducted to identify the cause. For example, in a software driven device, the failure may be related to the device design, the manufacturing process, or the quality assurance equipment used in the evaluation of the device. In a device that consists only of software, the cause of the failure may be related to the software design or the process used for duplicating the software. When the failure of a finished device is attributable to the software used in manufacturing or quality assurance, identification of the cause of a failure may require review of the software program's logic and of the test procedures and results, as well as a retesting of the program. Further reviews may be required of the duplication process and of environmental control records for those areas where ESD sensitive components were handled and assembled.

If the software error is in the device, similar investigative activities are conducted. In either situation, the investigation extends to determining effects on other products, and results in a written record of the investigation and any follow-up action and corrective action taken.

4.12 Records, General Requirements (820.180)

Recordkeeping requirements that apply to nonautomated devices also apply to software controlled devices. Records must be available for review and copying by FDA employees, including those records which have been computerized and placed on computer storage media such as magnetic tape, disks, etc.

All records maintained in accordance with 21 CFR 820 are required to be retained for a period of time equivalent to the design and expected life of the device, but in no case less than two years from the date of release of the device for commercial distribution.

4.13 Device Master Record (820.181)

The device master record (DMR) consists of diagrams, descriptions, schematics, etc., that constitute the specifications for the medical device product, the manufacturing process, and QA program. In addition to items detailing specifications for the device hardware, the device master record for a software driven product also includes detailed specifications for the device software. Detailed specifications are also required when the device consists of only software.

All records and documents contained in the device master record are controlled documents, including documentation related to software. Any revision or change of the software program or its supporting documentation are made in accordance with formal change control procedures and authorized by signature of the designated individual(s). Magnetically coded badges and other electronic identifiers may be used in lieu of signatures if adequate controls are in place to prevent their misuse.

4.13.1 Specifications (820.181(a))

The device master record must include specifications for the device. When software is part of the device, specifications include or refer to:

- the final, complete, approved software design requirements, which describe in narrative and/or pictorial form, such as a flow chart, what the software is intended to do (e.g., to control or monitor something) and how it will accomplish these tasks. Also included is a description of how the software will interact with the hardware to

accomplish various functions of the device's design. The specifications may also include a checksum for the program. The description is in a form that can be understood by all individuals who work on and/or will maintain the program during its life. Note that the description does not include documentation of the working drafts (or in-process steps) of the software design; it only includes the final approved specifications. The procedures for evaluation of the software to assure specifications are met are covered by 820.181(c).

- a description of the device's computer hardware system specifications, such as interfaces, connections, and media for storage of the program in the device.

- the computer source code as either hard copy or on magnetic medium. It usually is necessary for the finished device manufacturer to have the source code. This documentation is indispensable for adequately maintaining the program and evaluating the impact of any change on the rest of the program.

  It is important that the device manufacturer collaborate with the software vendor in the initial stages when software specifications are being developed and when any changes are introduced in order to assure that the intent of the design is adequately translated into software code. In these situations, the device manufacturer and software vendor establishes a contract that delineates responsibilities relating to the development and maintenance of the software.

The program source code typically includes or refers to adequate documentation which describes the subroutines or modules for the language used. Additional documentation that describes the design of the program is maintained. The intent is to assure that individuals maintaining the program have sufficient documentation to fully understand the purpose of the software design. Depth and detail of the documentation are proportionate to the complexity of the systems involved.

4.13.2 Production Process Procedures (820.181(b))

The DMR must contain production process specifications. When applied to software controlled processes the DMR includes procedures for environmental control and specifications where applicable; procedures for duplication of software for assembly into the finished device; specifications for use of any automated or

computerized manufacturing equipment or processes; and specifications for any computerized packaging and labeling operations. The DMR also includes procedures for computer/software security, if implemented.

To assure consistency of results, the DMR includes written change control procedures and any change in software that is part of the device or that is used in manufacturing or in quality assurance.

4.13.3 Quality Assurance Procedures and Specifications (820.181(c))

The DMR must also include all documentation used to determine quality of conformance to established specifications for the components, device, packaging, labeling and manufacturing processes. For software, this includes, but is not limited to, identification of any automated test equipment, as well as test procedures and criteria used to evaluate the current device software program for acceptance for use in manufacturing (820.80)(a) and for acceptance of hardware components used to store the software in the device (also 820.80(a)). For computerized manufacturing processes, this also includes any tests which are performed to evaluate the adequacy of the process, such as evaluating the integrity of package seals and verifying that the correct label was applied.

4.13.4 Labeling (820.181(d))

The final element required by the device master record concerns labeling for the finished medical device. Because of the possible complexity of a software driven device, extensive labeling may be required for adequate user instructions. This labeling may take the form of user manuals or it may be embedded directly into the software for the device, appearing on screen as instructions and menus.

User manuals or directions are written in clearly understood terminology and consist of operating instructions that explain how the system works and the procedures to be followed. Manuals include an explanation of all advisories, alarm and error messages, as well as corrective actions to be taken when these situations occur.

4.14 Device History Record (820.184)

The device history record (DHR) demonstrates that the device is manufactured in accordance with the specifications in the device master record. This agreement is shown by documented evidence

that manufacturing and test procedures have been followed and that the results meet acceptance criteria. When software is part of the device, this documentation includes a record of the version of the software which was assembled into the device, results from evaluating the device software (e.g., performance), in addition to all documentation needed to show that the software was adequately reproduced during manufacturing.

Adequate production records are in place to properly document all significant activities. For example, software that is part of a device may be copied into components, such as PROMs (Programmable Read Only Memory Chips), which are then assembled into the device. Production records for this activity document the results of the duplication process. For example, when checksums are used to identify the revision of the software which is duplicated into components, the production record documents the checksum and the number of components which were copied as well as the date the activity was performed. All production records are included in, or referred to in, the device history record.

4.15 Critical Devices, Automated Data Processing (820.195)

Section 820.195 applies only to manufacturing or quality assurance activities associated with critical devices. Automated data processing is the means used to gather and analyze information on some characteristic of the device manufacturing process or QA program without direct use of an operator to control the activity or verify the results. Automated data processing systems provide an effective method for performing routine, repetitive tasks. Although generally more reliable than manual equivalents, such systems demand adequate controls for equipment setup and programming. The GMP regulation requires a manufacturer to implement controls that will assure the correctness and appropriateness of these programs, program changes, equipment and data input and output.

4.16 Complaint Files (820.198)

Firms must prepare and implement adequate complaint handling systems including the review, investigation, and evaluation of both hardware and software failures of distributed devices. A notation in the complaint file that a system has failed as a result of a software error is supported with data or evidence to justify that conclusion. When a software failure is encountered, an investigation is conducted to determine the cause of the error and its impact on the capabilities of the device and similar devices.

Many manufacturers use computers for recording and tracking complaint information contained in paper documents, such as letters from complainants or laboratory reports. The complete information may be copied into the computer system in lieu of

maintaining the original documents. If the documents are retained, however, the computerized complaint record makes reference to corresponding paperwork.

Complaints are an excellent source of information about device design and the manufacturing process by which the device was produced. When complaint files are computerized, a software program that provides a means of determining the existence of any similar recurring problems with the device, similar devices, or with the manufacturing process, which might indicate a need for possible corrective action, is invaluable.

- END -

APPENDIX A

DEFINITIONS

Archived Master (copy of software)	A software library which contains formally approved and released versions of software and documentation from which copies are made.
Checksum	The value from adding the individual values at each address of the hardware component which contains the software program. This value may also be used to indicate software versions.
Chips	An electronic hardware component consisting of integrated microcircuits which perform a significant number of functions.
Disk Directories	Index of the file names on the disk. It may also include file size, date of creation, and date last altered.
Electrostatic Discharge (ESD)	A discharge of the potential energy that electric charges possess by virtue of their positions relative to each other. This discharge may adversely affect hardware sensitive to potential differences.
Error Checking	A means of determining if recording of data, its input into a computer system, and its transfer within the system, including transmission, is correct.
Fault Tolerance	Systems that continue to operate satisfactorily in the presence of faults (i.e., hardware failures).
Integrated Circuits (IC)	Complex electronic circuits etched on small semiconductor chips.
Master Copies of Software	The approved versions of the software from which copies are made for use and reproduction in the manufacturing environment.
Polling	In a data communications system, a line control method in which the computer asks each terminal on the system, in turn, if it has a message to send.
Programmable Read Only Memory Chips (PROMS)	Memory chips of which the contents can be read but not altered during program execution. However, the contents of the memory can be altered before it is assembled in the computer system.

PROM Programmer	Electronic equipment which is used to transfer a software program into a PROM.
Third-Party Certification	The procedure and action, by a duly authorized independent body, of confirming that a system, software subsystem, or computer program is capable of satisfying its specified requirements in an operational environment. Certification usually takes place in the field under actual or simulated operational conditions, and is used to evaluate the software itself and the specifications to which the software was designed. Certification activities take place under a written, approved (by the manufacturer) protocol.
Validation	Establishing documented evidence which provides a high degree of assurance that a specific process will consistently produce a product meeting its predetermined specifications and quality attributes.
Validation Testing	Testing that commences after the completion of the development testing and includes module and subsystem level testing. These tests can be considered to be "rehearsals;" they are basically gross tests of the coding against specifications.
Verification	The process of reviewing, inspecting, testing, checking, auditing, or otherwise establishing and documenting whether or not items, processes, services, or documents conform to specified requirements.
Verification Testing	An acceptance test of software. These tests are rigorous and detailed and will result in the software quality certification that the coding is in complete agreement with the specifications, design, and test documentation.
Worst Case	A set of conditions encompassing upper and lower processing limits and circumstances, including those within standard operating procedures, which pose the greatest chance of process or product failure when compared to ideal conditions. Such conditions do not necessarily induce product or process failure.

APPENDIX B

REFERENCES

1. FDA 84-4191: Medical Device GMP Guidance for FDA Investigators (April 1984).

2. FDA Compliance Policy Guides

   Office of Enforcement, Compliance Policy Guide 7132A.07: Computerized Drug Processing: Input/Output Checking (October 1, 1982).

   Office of Enforcement, Compliance Policy Guide 7132A.08: Computerized Drug Processing; Identification of "Persons" on Batch Production and Control Records, (December 1, 1982).

   Office of Enforcement, Compliance Policy Guide 7132A.11: Computerized Drug Processing., CGMP Applicability to Hardware and Software, (December 1, 1984).

   Office of Enforcement, Compliance Policy Guide 7132A.12: Computerized Drug Processing., Vendor Responsibility, (January 18, 1985).

   Office of Enforcement, Compliance Policy Guide 7132A.15: Computerized Drug Processing; Source Code for Process Control Application Programs, (April 16, 1987).

3. FDA 84-4191: Software Development Activities, Reference Materials and Training Aids for Investigators (July 1987).

4. FDA Field Computer Specialists and their location: Martin Browning, DFI/ORA, Rockville, MD; John Kunkel, Minneapolis District; Philip Piasecki, Boston District; Sam Clark, Atlanta District; Paul Figarole, Baltimore District; Dwight Herd, San Juan District.

5. References for Definitions:

   Capron, H.L. and Williams, Brian K., Computers and Data Processing, 1982, The Benjamin/Cummings Publishing Company, Inc.

   Parker, Sybil P., Editor-in-Chief, McGraw-Hill Dictionary of Scientific and Technical Terms, 1984, McGraw-Hill Book Company.

   Ralston, Anthony, Editor, Encyclopedia of Computer Science and Engineering, 1983, Van Nostrand Reinhold Company.

   Foster, Richard A., Introduction to Software Quality Assurance, 1975, R. A. Foster.

Dersey, Roger M., Digital Circuits and Devices, 1985, John Wiley and Sons, Inc.

Fraf, Rudolf F., Modern Dictionary of Electronics, 1977, Howard W. Sams and Company, Inc.

Jay, Frank, Editor-in-Chief, IEEE Standard Dictionary of Electrical and Electronics Terms, 1984, The Institute of Electrical and Electronics Engineers, Inc.

6. Recommended References:

FDA 87-4179: CDRH, Device Good Manufacturing Practices Manual, 4th Edition, Division of Small Manufacturers Assistance, OTA (November 1987).

FDA Compliance Program Guidance Manual, Compliance Program 7382.830, Inspection of Medical Device Manufacturers (October 1985).

Center for Drugs and Biologics and Center for Devices and Radiological Health, Guideline on General Principles of Process Validation (May 1987).

FDA 90-4236: CDRH, Preproduction Quality Assurance Planning; Recommendations for Medical Device Manufacturers, Office of Compliance and Surveillance, Division of Compliance Programs (September 1989).