21 CFR 820

Orlando López – Rev 03-Sep-11

www.computer-systems-validation.com

The following matrix outlines the applicability the medical devices QSR to the computer systems on manufacturing, quality assurance, and/or recordkeeping. It also applies to manufacturers of medical devices that are driven or controlled by software or software medical devices.

The origin of this matrix is the outdated May 1992 US FDA Computerized Devices/Processes Guidance – Application of the Medical Device GMP to Computerized Devices and Manufacturing Processes. The references in the outdated guideline were updated using the US FDA QSR Regulation (October 1996) and the QSR Guidebook for Medical Devices[1]. Additional references are from the General Principles of Software Validation; Guidance for Industry and FDA Staff. (January 2002) and EU Crosswalk (www.computer-systems-validation.com).

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
820.3(z) and (aa) 820.30(f) and (g)	Validation Verification Design Verification Design Validation	A documented software requirements specification provides a baseline for both validation and verification. The software validation process cannot be completed without an established software requirements specification
820.20(b)(1) and (2)	Responsibility and Authority	• Management must identify and provide the appropriate software development environment and resources. • There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties. (EU Annex 11-2)
820.20(b)(3)	Management Representative	QA software checks may be both quantitative and qualitative; testing is not restricted to quantitative measurements. Testing of software involves evaluation of conformance to specifications and ability to perform as intended.
820.20(c)	Management Review	Computer systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status report(s). (EU Annex 11-11)
820.22	Quality Audits	It is required manufacturers to conduct planned and periodic audits of their quality assurance program. This audit includes evaluation of procedures used to assure that hardware and software are adequate for their intended use, and that all procedures remain adequate. The audits extend to all phases of software design transfer, implementation, testing, and maintenance activities related to computerized processes and devices.
820.25(b)	Training	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

[1] K. Trautman, "The FDA and Worldwide Quality System Requirements Guidebook for Medical Devices," ASQ Quality Press, Milwaukee, Wisconsin, 1997.

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
		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.
820.30	Design Controls	Medical device software product developed after June 1, 1997, regardless of its device class, is subject to applicable design control provisions[2].
820.30(c)	Design Inputs	Requires a mechanism for addressing incomplete, ambiguous, or conflicting requirements.
820.30(g)	Design Validation	The device software (embedded software) in a medical device is validated to assure it performs as intended. (**Note**: Look at the end of this table for advise on validation by the US FDA)
820.30(h)	Design Transfer	Manufacturers are prepared to provide evidence that the software used for duplicating the device software, and the software used in automated manufacturing or QA, meet the software design specifications.
820.40 820.30(i). 820.70(i)	Document Control Design Changes Automated Processes	Any changes to a computer system including system configurations should only be made in a controlled manner in accordance with a defined procedure. (EU Annex 11-10)
820.50	Purchasing Controls	• When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computer system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous. (EU Annex 11-3.1) • The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment. (EU Annex 11-3.2) • Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled. (EU Annex 11-3.3) • Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request. (EU Annex 11-3.4)
820.70(a)	Production and process controls	• When the possibility exists for the device to deviate from its design specifications as a result of an inadequately controlled manufacturing process, it is required that written

[2] O. López, "*Applying Design Controls to Software in the FDA-Regulated Environment,*" Journal of cGMP Compliance, July 1997.

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
		manufacturing procedures must be established. • Standard operating procedures 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 and passkeys. Assignment and use of these security measures should also be controlled.
820.70(a) 820.184 820.180	Production and process controls	Computer systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. (EU Annex 11-5)
820.70(c)	Environmental Controls	Computers and software storage media may be sensitive to the environment. 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. Other environmental conditions to be considered are: humidity, electrostatic discharge (ESD) and electro-magnetic interference (EMI).
820.70(g)	Equipment	Manufacturing equipment must meet specified requirements.
820.70(g)	Equipment	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.
820.70(i)	Automated Processes	The GMP regulation requires the medical device manufacturer to implement controls that will assure the correctness and appropriateness of computer systems, computer system changes, equipment, and data input and output.

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
		When a manufacturing process is automated; the computer 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: • equipment (e.g., peripheral) and sensor checks using known inputs, which may consist of processing test or simulated data; • alarm checks at, within, and beyond their operational limits; and, evaluation of operator override mechanisms for how they are used by operators and how they are documented. The software validation requirement also applies to automated tools used to design medical devices and tools used to develop software (e.g., computer-aided design and software development tools). Refer to comment #136 in the preamble to the Quality System Regulation (61 FR 52630).
820.70(i)	Automated Processes	When automated production (software used to automate any part of the device production processor) or QA systems (software used to automate any part of the quality system) are used, the software programs are validated. This requirement applies to any software used to automate device design, testing, component acceptance, manufacturing, labeling, packaging, distribution, complaint handling, or to automate any other aspect of the quality system. Validation must occur before use of the computer system.
11.10(a)	Automated Processes (e-recs)	Computer systems used to create, modify, and maintain electronic records and to manage electronic signatures are also subject to the validation requirements. Such computer systems must be validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
820.70(i)	Automated processes (Modifications)	Validation may also be required after significant revision of the system occurs and after any revision of the operating system software. 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

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
		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 is 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.
820.70(i)	Automated Processes (Modifications)	If the change significantly extends the indication for use, or affects the safety or effectiveness of the device, a new 510(k) Premarket Notification or Premarket Approval 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. References: a) Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 2005. b) 510(k) Device Modifications: Deciding When to Submit a 510(k)for a Change to an Existing Device, DRAFT July 2011.
820.75 and 820.70(i)	Process Validation and Automated Processes	When software is involved in manufacturing and quality assurance an evaluation is performed. This evaluation is performed when software is developed in-house and when it has been supplied by a vendor.
820.80(a)	Receiving, in-process, and finished device acceptance General	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. 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. This section applies to both hardware and software components that are critical. Hardware may include custom designed components (e.g., 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

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
		supplier makes any changes because a change to a component may adversely impact the finished device. Proposed changes are evaluated .to determine the effect on the device's conformance with specifications.
820.80(b)	Receiving acceptance activities	The software is evaluated to assure the unused portions do not interfere with proper performance.
820.80(d)	Final acceptance activities	• Adequate written 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. 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. • 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.
820.80(e)	Acceptance records	A manufacturer's QA program includes procedures for assuring approval or rejection of contract-supplied software for incorporation into medical devices, control of manufacturing

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
		processes, and use in quality assurance activities.
820.80(e)	Acceptance records	If a computerized device is a critical device, and it does not meet its performance specifications during finished device inspection, an adequate investigation must be conducted to identify the cause. 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. In a software driven device, the failure may be related to the software design, some other aspect of the device design, the process used for duplicating the software, some other step in the manufacturing process, or the quality assurance equipment or software used in evaluation of the device. Failure related to software design may require review of the software program logic and retesting of the program. Review may be required of the process for duplicating the software. It may be appropriate to review environmental control specifications and monitoring records for those areas where Electrostatic Discharge (ESD) sensitive components were handled and assembled. The investigation extends to determining effects on other products. A written record is made of the investigation findings and any follow—up and corrective action taken.
820.100	Corrective and preventive actions	Where trends are identified (e.g., recurrence of similar software anomalies), appropriate corrective and preventive actions must be implemented and documented to avoid further recurrence of similar quality problems.
820.100	Corrective and preventive actions	When a failure occurs after the distribution of software driven device, or a device which consists solely of software, an adequate investigation must be conducted to identify the cause. The approach to investigating distributed devices which have failed is similar to the approach described in the preceding section for investigating critical devices which fail finished device testing. The investigation extends to determining effects on other products. A written record is made of the investigation, including conclusions and follow up, or corrective action taken.
820.120	Device Labeling	Screen displays (which provide instructions to the user of a computer controlled device) and written user manuals are considered device labeling. Such labeling is reviewed and examined for accuracy and adequacy. A record of the date of the labeling review, and the person performing the review, is maintained in the device history record (DHR).
820.170	Installation	Testing at the user site is a vital part of software validation. Requires installation and inspection procedures (including testing where appropriate) as well as documentation of

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
		inspection and testing to demonstrate proper installation.
820.180	Recordkeeping requirements	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, and optical storage media). All records maintained in accordance with 21 CFR Part 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. Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. (EU Annex 11-7.1) Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically. (EU Annex 11-7.2)
820.181	Device Master Records	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, as well as an evaluation to assure it performs as intended.
820.181	Device Master Records	The DMR for a software driven product also includes detailed specifications for the device software. Detailed specifications are also required when the device consists-only software. All records and documents contained in the DMR are controlled. Any revision or change of the software program, or its supporting documentation, is made in accordance with formal change control procedures and is authorized by signature of the designated individual(s). Electronic identifiers may be used instead of signatures if they provide a high degree of security, are validated, and adequate controls are in place to prevent their misuse.
820.181(a)	Device Specifications within the DMR	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

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
		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 is usually 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 establish 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 directly proportional to the complexity of the systems involved.
820.181(b)	Production Process Procedures within the DMR	For 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. Any change in software that is part of the device, or that is used in manufacturing or in QA, is subject to change control procedures. The DMR is updated when changes are made So that it contains current specifications, procedures, and versions.
820.181(c)	Quality Assurance Procedures and Specifications within the DMR	Identification of any automated test equipment, as well as test procedures and criteria, used to evaluate the current device software program for acceptance of hardware components used to store the software in the device. For computer manufacturing processes, this also includes any tests which are performed to determine the adequacy of the process, such as evaluating the integrity of package seals and

CFR #	CFR Title	Impact of CFR on Computer System in Medical Devices regulations
		verifying that the correct label was applied.
820.181(d)	Labeling	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, alarms, and error messages, as well as corrective actions to be taken when these situations occur.
820.184	Device History Record (DHR)	Mandates that all production computer records must be reviewed.
820.184	Device History Records	When software is part of the device, this documentation (manufacturing and testing procedures have been followed, and that the results meet acceptance criteria) includes a record of the version of the software which was assembled into the device and 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. For example: 1) Software that is part of a device may be copied into components, such as PROMs, which are then assembled into the device. Production records for this activity document the results of the duplication process. 2) 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, or referred to, in the DHR.
820.198	Complaint Files	It is required establishing adequate complaint handling systems which include 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.

Medical Device Software Validation[3] (820.30(g))

Software is evaluated and reviewed versus the software specifications during the ongoing development of the device design. When a "final" prototype(s) is available, the software and hardware are validated to make certain manufacturer specifications for the device and process are met. Some aspects of hardware evaluation were discussed above. Aspects specific to software are covered below.

Before testing the software in actual use, the detailed code should be visually reviewed versus flow charts and specifications. All cases, especially decision points and error/limit handling, should be reviewed and the results documented.

In all cases, algorithms should be checked for accuracy. Recalls have occurred because algorithms were incorrectly copied from a source and, in other cases, because the source algorithm was incorrect. During the development phase, complex algorithms may need to be checked by using a test subroutine program written in a highorder language, if the operational program is written in a lowlevel language.

The validation program is planned and executed such that all relevant elements of the software and hardware are exercised and evaluated. The testing of software usually involves the use of an emulator and should include testing of the software in the finished device.

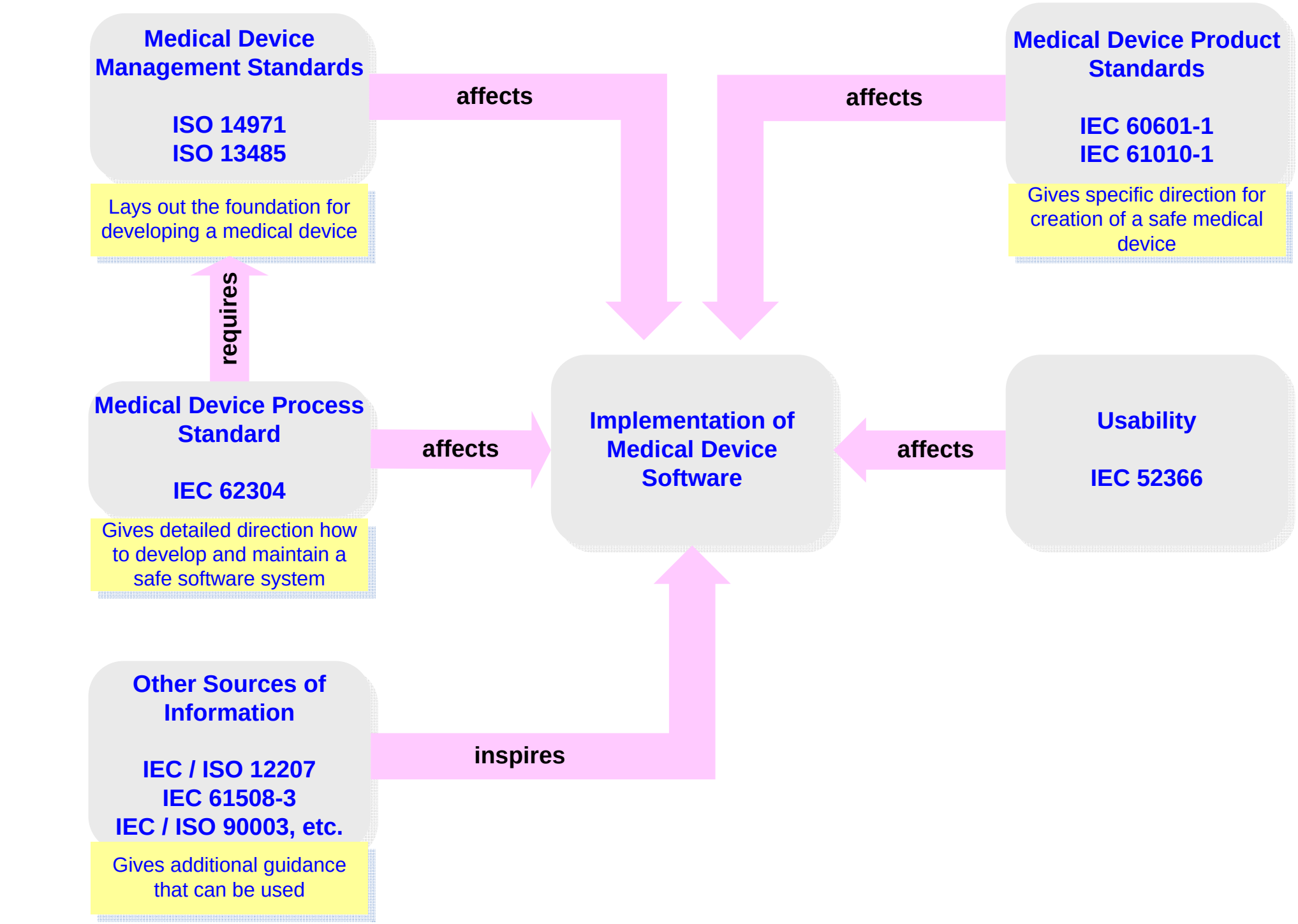
The testing includes normal operation of the complete device; and this phase of the validation program may be completed first to make certain that the device meets the fundamental performance, safety and labeling specifications. Concurrently or afterward, the combined system of hardware and software should be challengedwith abnormal inputs and conditions. As appropriate, these inputs and conditions include such items as:

- operator errors;
- induced failure of sensors and cables or other interconnects;
- induced failure of output equipment;
- exposure to static electricity;
- power loss and restart;
- simultaneous inputs or interrupts; and,
- as appropriate, deliberate application of none, low, high, positive, negative, and extremely high input values.

The results of the software and combined device system validation are included in the design reviews.

---

3 US FDA, Medical Device Quality Systems Manual: A Small Entity Compliance Guide, **April 14, 1999**


Medical Device Management Standards
ISO 14971
ISO 13485
Lays out the foundation for developing a medical device
affects
Medical Device Product Standards
IEC 60601-1
IEC 61010-1
Gives specific direction for creation of a safe medical device
affects
requires
Medical Device Process Standard
IEC 62304
Gives detailed direction how to develop and maintain a safe software system
affects
Implementation of Medical Device Software
affects
Usability
IEC 52366
Other Sources of Information
IEC / ISO 12207
IEC 61508-3
IEC / ISO 90003, etc.
Gives additional guidance that can be used
inspires

Disclaimers.

The recommendations to implement 21 CFR 820, as described in the above matrix, are purely from the standpoint and opinion of the author, and should serve as a suggestion only. They are not intended to serve as the regulators' official implementation process.

The information contained here is provided in good faith and reflects the personal views of the author. No liability can be accepted in any way. The information provided does not constitute legal advice.

Revision History

3-Sep-11	Creation of the matrix correlating of Computer Systems and Medical Devices QSR.
6-Sep-11	Added ISO standards relationship model v0, provided by Siegfried Schmitt, Siegfried.Schmitt@parexel.com.