

Definitions, Regulations and Guidance

For

Change Control and Configuration Management

for GXP Computerised Systems

Document Prepared By:

R.D.McDowall
Principal,
McDowall Consulting, UK

Document Version: 1.0

Date: 17th August 2005

Table of Contents

1	CHANGE MANAGEMENT DEFINITIONS	3
2	GOOD LABORATORY PRACTICE REGULATIONS AND GUIDANCE	6
2.1	FDA GLP (21 CFR 58).....	6
2.2	OECD GLP CONSENSUS DOCUMENT 1995.....	6
2.3	SWISS AGIT GLP GUIDANCE FOR COMPUTERISED SYSTEMS.....	7
3	GOOD MANUFACTURING PRACTICE	8
3.1	21 CFR 211 – CURRENT GOOD MANUFACTURING PRACTICES FOR FINISHED PHARMACEUTICAL PRODUCTS.....	8
3.2	§425.100 COMPUTERIZED DRUG PROCESSING; CGMP APPLICABILITY TO HARDWARE AND SOFTWARE* (CPG 7132A.11)	9
3.3	GOOD MANUFACTURING PRACTICE FOR MEDICINAL PRODUCTS IN THE EUROPEAN COMMUNITY - GMP GUIDE ANNEX 11: COMPUTERISED SYSTEMS.....	10
3.4	ICH Q7A GOOD MANUFACTURING PRACTICE FOR ACTIVE PHARMACEUTICAL INGREDIENTS	13
3.5	§820.70 PRODUCTION AND PROCESS CONTROLS.	14
4	GOOD CLINICAL PRACTICE.....	16
4.1	ICH HARMONISED TRIPARTITE GUIDELINE FOR GCP.....	16
4.2	COMPUTERISED SYSTEMS IN CLINICAL TRIALS – 1999 VERSION	16
4.3	COMPUTERISED SYSTEMS IN CLINICAL TRIALS – 2004 VERSION	16
4.4	COMPUTERISED SYSTEMS VALIDATION IN CLINICAL RESEARCH	17
5	PIC/S GUIDANCE: COMPUTERISED SYSTEMS IN GXP ENVIRONMENTS	19
5.1	§17. CHANGE MANAGEMENT	19
5.2	§18. CHANGE CONTROL AND ERROR REPORT SYSTEM.....	19
6	GENERAL PRINCIPLES OF SOFTWARE VALIDATION.....	21
6.1	§4.7. SOFTWARE VALIDATION AFTER A CHANGE	21
6.2	§5.2.7. MAINTENANCE AND SOFTWARE CHANGES	21
7	NIST SPECIAL PUBLICATION 800-40 – HANDLING SECURITY PATCHES	23
7.1	EXECUTIVE SUMMARY.....	23
7.2	DOCUMENT STRUCTURE.....	24
8	ISO 17799 INFORMATION SECURITY MANAGEMENT.....	25
8.1	§8.1.2 OPERATIONAL CHANGE CONTROL.....	25
8.2	§10.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	25
9	CYBERSECURITY FOR NETWORKED MEDICAL DEVICES CONTAINING OFF-THE-SHELF (OTS) SOFTWARE	28
9.1	INTRODUCTION	28
9.2	THE LEAST BURDENSOME APPROACH	28
9.3	BACKGROUND.....	28
	QUESTIONS AND ANSWERS	29

1 Change Management Definitions

The definitions below have been abstracted and adapted from the

- IT Infrastructure Library (ITIL) publication “Service Delivery”
- IEEE Standard 610 (Glossary)
- NAMAS (now UKAS) Guidance NIS37, A Guide to managing the Configuration of Computer Systems (Hardware, Software and Firmware) used in NAMAS Accredited Laboratories.

Note that there can be more than one definition for the same term and that there may be differences between these definitions.

Term	Definition(s)
Change	The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation (ITIL).
Change Advisory Board	A group of people who can give expert advice to Change management on the implementation of Changes. This board is likely to be made up of representatives from all areas within IT and representatives from business units (ITIL).
Change Authority	A group that is given the authority to approve Change. Sometimes called the Configuration Board (ITIL).
Change Control	<p>The procedure to ensure that all Changes are controlled, including the submission, analysis, decision making, approval, implementation and post-implementation of the Change (ITIL).</p> <p>A formal process by which qualified representatives from appropriate disciplines review proposed or actual changes to a computer system. The main objective is to document the changes and ensure that the system is maintained in a state of control (PDA).</p>
Change Document	Request for Change, Change control form, Change order, Change record (ITIL).
Change History	Auditable information that records, for example, what was done, when it was done by who and why (ITIL)
Change Log	A log of Requests for Change raised during the project, showing information on each Change, its evaluation, what decisions have been made and its current status e.g. raised, reviewed, approved, implemented, closed (ITIL).
Change Management	Process of controlling Changes to the system or any aspect of services, in a controlled manner, enabling approved Changes with minimum disruption (ITIL).
Change Record	A record containing details of which Configuration Items are affected by an authorised Change (planned or implemented) and how (ITIL).

Configuration	<p>(1) The arrangement of a computer system or component as defined by the number, nature, and interconnections of its constituent parts (IEEE).</p> <p>(2) In configuration management, the functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product (IEEE)</p>
Configuration Baseline	Configuration of a system established at a specific point in time, which captures the structure and details of the system and enables that system to be rebuilt at a later date (ITIL).
Configuration Control	<p>Activities comprising the control of Changes to Configuration Items after formally establishing its configuration documents. It includes the evaluation, co-ordination, approval, approval or rejection of Changes. The implementation of Changes includes changes, deviations and waivers that impact on the configuration (ITIL).</p> <p>An element of configuration management, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification. <i>Synonym:</i> change control (IEEE).</p>
Configuration Control Board (CCB).	A group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes. <i>Synonymous:</i> change control board. (IEEE)
Configuration Documentation	Documents that define requirements, system design, build, production and verification for a configuration item (ITIL).
Configuration Identification	<p>Activities that determine the system structure, the selection of Configuration Items, and the documentation of the Configuration Items' physical and functional characteristics including interfaces and subsequent Changes. It includes the allocation of identification characters and numbers to the Configuration Items and their documents. It also includes the unique numbering of configuration control forms associated with Changes and Problems (ITIL).</p> <p>(1) An element of configuration management, consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation (IEEE).</p> <p>(2) The current approved technical documentation for a configuration item as set forth in specifications, drawings, associated lists, and documents referenced therein (IEEE).</p>
Configuration Index.	A document used in configuration management, providing an accounting of the configuration items that make up a product (IEEE).

Configuration Item (CI)	<p>Component of an infrastructure or system or an item such as Request for Change which is under the control of Configuration Management. Configuration Items may vary widely in complexity, size and type – from an entire system (including all hardware, software and documentation) to a single module or a minor hardware component (ITIL)</p> <p>An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process (IEEE).</p>
Configuration Management	<p>The system for identifying the configuration of hardware, software, firmware or documentation at discrete points in time with the purpose of systematically controlling changes to the configuration and maintaining the integrity and traceability of the configuration throughout the system life cycle (NIS37).</p> <p>A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. (IEEE).</p>
Configuration Status Accounting	<p>An element of configuration management, consisting of the recording and reporting of information needed to manage a configuration effectively. This information includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes. (IEEE)</p>

2 Good Laboratory Practice Regulations and Guidance

2.1 FDA GLP (21 CFR 58)

§58.63 Maintenance and Calibration of Equipment

(a) Equipment shall be adequately inspected, cleaned, and maintained. Equipment used for the generation, measurement, or assessment of data shall be adequately tested, calibrated and/or standardised.

(b) The written standard operating procedures required under paragraph 58.81(b)(11) shall be set forth in sufficient detail the methods, materials, and schedules to be used in the routine inspection, cleaning, maintenance, testing, calibration, and/or standardisation of equipment, and shall specify, when appropriate, remedial action to be taken in the event of failure or malfunction of equipment. The written standard operating procedures shall designate the person responsible for the performance of each operation.

(c) Written records shall be maintained of all inspection, maintenance, testing, calibration and/or standardising operations. These records, containing the date of the operation, shall describe whether the maintenance operations were routine and followed the written standard operating procedures. **Written records shall be kept of non-routine repairs performed on equipment as a result of failure and malfunction. Such records shall document the nature of the defect, how and when the defect was discovered, and any remedial action taken in response to the defect.**

2.2 OECD GLP Consensus Document 1995

§7 Validation of Computerised Systems - c) Change Control

Change control is the formal approval and documentation of any change to the computerised system during the operational life of the system. Change control is needed when a change may affect the computerised system's validation status. Change control procedures must be effective once the computerised system is operational.

The procedure should describe the method of evaluation to determine the extent of retesting necessary to maintain the validated state of the system. The change control procedure should identify the persons responsible for determining the necessity for change control and its approval.

Irrespective of the origin of the change (supplier or in-house developed system), appropriate information needs to be provided as part of the change control process. Change control procedures should ensure data integrity.

2.3 Swiss AGIT GLP Guidance for Computerised Systems

§ 8.2 Standard Operating Procedures

The OECD consensus document #10 requires a set of standard operating procedures for the development and/or routine use of validated computerised systems; they include SOPs for

Operation

In addition to the User's Manual, this SOP describes how the application will be used in a particular laboratory. When the user has the opportunity to customise a system for his particular needs, this has to be specified. Furthermore, the SOP will contain information on who is the system administrator, and it will reference other pertinent SOPs to be followed when using the system.

Security

Three levels of security must be addressed: physical security of the system [server(s) and workstation(s)]; logical access to the application; and logical access to the operating system including access to data and program files for the application.

Change Control

Effective change management is the single most important factor in maintaining a validate state for a production system. All forms of change must be tracked and managed. This will always include application software updates, operating system updates, and changes to the hardware running the application.

Depending upon the type of system being validated, this may include changes to the network or modification to a qualified workstation. Every change, no matter how minor, must be evaluated for its potential impact on the validated application as defined in a change control SOP.

3 Good Manufacturing Practice

3.1 21 CFR 211 – Current Good Manufacturing Practices for Finished Pharmaceutical Products

§ 211.63 Equipment Design, Size, and Location

Equipment used in the manufacture, processing, packing, or holding of a drug product shall be of appropriate design, adequate size, and suitably located to facilitate operations for its intended use and for its cleaning and maintenance.

§ 211.68 Automatic, Mechanical, and Electronic Equipment

(a) Automatic, mechanical, or electronic equipment or other types of equipment, including computers, or related systems that will perform a function satisfactorily, may be used in the manufacture, processing, packing, and holding of a drug product. If such equipment is so used, it shall be routinely calibrated, inspected, or checked according to a written program designed to assure proper performance. Written records of those calibration checks and inspections shall be maintained.

(b) **Appropriate controls shall be exercised over computer or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel.** Input to and output from the computer or related system of formulas or other records or data shall be checked for accuracy. The degree and frequency of input/output verification shall be based on the complexity and reliability of the computer or related system. A backup file of data entered into the computer or related system shall be maintained except where certain data, such as calculations performed in connection with laboratory analysis, are eliminated by computerization or other automated processes. In such instances a written record of the program shall be maintained along with the appropriate validation data. Hard copy or alternative systems, such as duplicates, tapes, or microfilm, designed to assure that backup data are exact and complete and that it is secure from alteration, inadvertent erasures, or loss shall be maintained.

3.2 §425.100 Computerized Drug Processing; CGMP Applicability to Hardware and Software* (CPG 7132a.11)

BACKGROUND:

The use of computers in the production and control of drug products is quickly increasing. Questions have been raised as to the applicability of various sections of the Current Good Manufacturing Practice Regulations to the physical devices (hardware) which constitute the computer systems and to the instructions (software) which make them function.

POLICY:

Where a computer system is performing a function covered by the CGMP regulations then, in general, hardware will be regarded as equipment and applications software¹ will be regarded as records. The kind of record (e.g., standard operating procedure, master production record) that the software constitutes and the kind of equipment (e.g., process controller, laboratory instrument) that the hardware constitutes will be governed by how the hardware and software are used in the manufacture, processing, packing, or holding of the drug product. Their exact use will then be used to determine and apply the appropriate sections of the regulations that address equipment and records.

¹ Applications software consists of programs written to specified user requirements for the purpose of performing a designated task such as process control, laboratory analyses, and acquisition/processing/storage of information required by the CGMP regulations.

Material between asterisks is new or revised

Issued: 10/19/84

Revised: 9/4/87

3.3 Good Manufacturing Practice For Medicinal Products In The European Community - GMP Guide Annex 11: Computerised Systems

Principle

The introduction of computerised systems into systems of manufacturing, including storage, distribution and quality control does not alter the need to observe the relevant principles given elsewhere in the Guide. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality and quality assurance. Consideration should be given to the risk of losing aspects of the previous system which could result from reducing the involvement of operators.

11.1 Personnel

It is essential that there is the closest co-operation between key personnel and those involved with computer systems. Persons in responsible positions should have the appropriate training for the management and use of systems within their field of responsibility which utilises computers. This should include ensuring that appropriate expertise is available and used to provide advice on aspects of design, validation, installation and operation of computerised system.

11.2 Validation

The extent of validation necessary will depend on a number of factors including the use to which the system is to be put, whether the validation is to be prospective or retrospective and whether or not novel elements are incorporated. Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and modifying.

11.3 System Environment

Attention should be paid to the siting of equipment in suitable conditions where extraneous factors cannot interfere with the system.

11.4 System Description

A written detailed description of the system should be produced (including diagrams as appropriate) and kept up to date. It should describe the principles, objectives, security measures and scope of the system and the main features of the way in which the computer is used and how it interacts with other systems and procedures.

11.5 Software Quality Assurance

The software is a critical component of a computerised system. The user of such software should take all reasonable steps to ensure that it has been produced in accordance with a system of Quality Assurance.

11.6 Automated Data Entry Verification & Checks

The system should include, where appropriate, built-in checks of the correct entry and processing of data.

11.7 IQ/OQ/PQ & Parallel Testing

Before a system using a computer is brought into use, it should be thoroughly tested and confirmed as being capable of achieving the desired results. If a manual system is being replaced, the two should be run in parallel for a time, as a part of this testing and validation.

11.8 System Security, Data Entry & Edits

Data should only be entered or amended by persons authorised to do so. Suitable methods of deterring unauthorised entry of data include the use of keys, pass cards, personal codes and restricted access to computer terminals. There should be a defined procedure for the issue, cancellation, and alteration of authorisation to enter and amend data, including the changing of personal passwords. Consideration should be given to systems allowing for recording of attempts to access by unauthorised persons.

11.9 Verification of Data Entry

When critical data are being entered manually (for example the weight and batch number of an ingredient during dispensing), there should be an additional check on the accuracy of the record which is made. This check may be done by a second operator or by validated electronic means.

11.10 Audit Trail of Data Edits

The system should record the identity of operators entering or confirming critical data. Authority to amend entered data should be restricted to nominated persons. Any alteration to an entry of critical data should be authorised and recorded with the reason for the change. Consideration should be given to building into the system the creation of a complete record of all entries and amendments (an "audit trail").

11.11 System Change Control

Alterations to a system or to a computer program should only be made in accordance with a defined procedure which should include provision for validating, checking, approving and implementing the change. Such an alteration should only be implemented with the agreement of the person responsible for the part of the system concerned, and the alteration should be recorded. Every significant modification should be validated.

11.12 Paper Copies for Quality Audits

For quality auditing purposes, it should be possible to obtain clear printed copies of electronically stored data.

11.13 Stored Data Protection & Retrieval

Data should be secured by physical or electronic means against wilful or accidental damage, in accordance with item 4.9. of the Guide. Stored data should be checked for accessibility, durability and accuracy. If changes are proposed to the computer equipment or its programs, the above mentioned, checks should be performed at a frequency appropriate for the storage medium being used.

11.14 Data Backup & Archive

Data should be protected by backing-up at regular intervals. Back-up data should be stored as long as necessary at a separate and secure location.

11.15 System Backup

There should be available adequate alternative arrangements for systems which need to be operated in the event of a breakdown. The time required to bring the alternative arrangements into use should be related to the possible urgency of the need to use them. For example, information required to effect a recall must be available at short notice.

11.16 Disaster Recovery

The procedures to be followed if the system fails or breaks down should be defined and validated. Any failures and remedial action taken should be recorded.

11.17 Error Tracking & Corrections

A procedure should be established to record and analyze errors and to enable corrective action to be taken.

11.18 Supplier Contracts

When outside agencies are used to provide a computer service, there should be a formal agreement including a clear statement of the responsibilities of that outside agency (see Chapter 7).

11.19 Batch Release & Qualified Person Security

When the release of batches for sale or supply is carried out using a computerised system, the system should allow for only a Qualified Person to release the batches and it should clearly identify and record the person releasing the batches.

NOTE: All words in italic are from original Annex 11 document. Titles next to numbers 11.3-11.19 have been added to facilitate reading.

3.4 ICH Q7A Good Manufacturing Practice for Active Pharmaceutical Ingredients

§5.4 Computerised Systems

5.40: GMP related computerised systems should be validated. The depth and scope of validation depends on the diversity, complexity and criticality of the computerised application.

5.41: Appropriate installation qualification and operational qualification should demonstrate the suitability of the computer hardware and software to perform assigned tasks

5.42: Commercially available software that has been qualified does not require the same level of testing. If an existing system was not validated at the time of installation, a retrospective validation could be conducted if appropriate documentation is available.

5.43: Computerised system should have sufficient controls to prevent unauthorised access or changes to data. There should be controls to prevent omissions in data (e.g. system turned off and data not captured). There should be a record to any data change made, the previous entry, who made the change and when the change was made.

5.44: Written procedures should be available for the operation and maintenance of computerised systems

5.45: Where critical data are being entered manually, there should be an additional check on the accuracy of the entry. This can be done by a second operator or by the system itself.

5.46: Incidents related to computerised systems that could affect the quality of intermediates or APIs or the reliability of records and test results should be recorded and investigated.

5.47: Changes to the computerised system should be made according to a change procedure and should be formally authorised, documented and tested. Records should be kept of all changes including modifications made to the hardware, software and any other critical component of the system. These records should demonstrate that the system is maintained in a validated state.

5.48: If system breakdowns or failures would result in the permanent loss of records a back-up system should be provided. A means of ensuring data protection should be established for all computerised systems.

5.49: Data can be recorded by a second means in addition to the computer system.

3.5 §820.70 Production and Process Controls.

(a) General. Each manufacturer shall develop, conduct, control, and monitor production processes to ensure that a device conforms to its specifications. Where deviations from device specifications could occur as a result of the manufacturing process, the manufacturer shall establish and maintain process control procedures that describe any process controls necessary to ensure conformance to specifications.

Where process controls are needed they shall include:

- (1) Documented instructions, standard operating procedures (SOP's), and methods that define and control the manner of production;
- (2) Monitoring and control of process parameters and component and device characteristics during production;
- (3) Compliance with specified reference standards or codes;
- (4) The approval of processes and process equipment; and
- (5) Criteria for workmanship which shall be expressed in documented standards or by means of identified and approved representative samples.

(b) Production and process changes. Each manufacturer shall establish and maintain procedures for changes to a specification, method, process, or procedure. Such changes shall be verified or where appropriate validated according to Sec. 820.75, before implementation and these activities shall be documented. Changes shall be approved in accordance with Sec. 820.40.

(c) Environmental control. Where environmental conditions could reasonably be expected to have an adverse effect on product quality, the manufacturer shall establish and maintain procedures to adequately control these environmental conditions. Environmental control system(s) shall be periodically inspected to verify that the system, including necessary equipment, is adequate and functioning properly. These activities shall be documented and reviewed.

(d) Personnel. Each manufacturer shall establish and maintain requirements for the health, cleanliness, personal practices, and clothing of personnel if contact between such personnel and product or environment could reasonably be expected to have an adverse effect on product quality. The manufacturer shall ensure that maintenance and other personnel who are required to work temporarily under special environmental conditions are appropriately trained or supervised by a trained individual.

(e) Contamination control. Each manufacturer shall establish and maintain procedures to prevent contamination of equipment or product by substances that could reasonably be expected to have an adverse effect on product quality.

(f) Buildings. Buildings shall be of suitable design and contain sufficient space to perform necessary operations, prevent mixups, and assure orderly handling.

(g) Equipment. Each manufacturer shall ensure that all equipment used in the manufacturing process meets specified requirements and is appropriately designed, constructed, placed, and installed to facilitate maintenance, adjustment, cleaning, and use.

(1) Maintenance schedule. Each manufacturer shall establish and maintain schedules for the adjustment, cleaning, and other maintenance of equipment to ensure that manufacturing specifications are met. Maintenance activities, including the date and individual(s) performing the maintenance activities, shall be documented.

(2) Inspection. Each manufacturer shall conduct periodic inspections in accordance with established procedures to ensure adherence to applicable equipment maintenance schedules. The inspections, including the date and individual(s) conducting the inspections, shall be documented.

(3) Adjustment. Each manufacturer shall ensure that any inherent limitations or allowable tolerances are visibly posted on or near equipment requiring periodic adjustments or are readily available to personnel performing these adjustments.

(h) Manufacturing material. Where a manufacturing material could reasonably be expected to have an adverse effect on product quality, the manufacturer shall establish and maintain procedures for the use and removal of such manufacturing material to ensure that it is removed or limited to an amount that does not adversely affect the device's quality. The removal or reduction of such manufacturing material shall be documented.

(i) Automated processes. When computers or automated data processing systems are used as part of production or the quality system, the manufacturer shall validate computer software for its intended use according to an established protocol. All software changes shall be validated before approval and issuance. These validation activities and results shall be documented.

4 Good Clinical Practice

4.1 ICH Harmonised Tripartite Guideline for GCP

§5.5 Trial Management, Data Handling and Record Keeping

§5.5.3 When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

- a. Ensure and document that the electronic data system(s) conforms to the sponsor's established requirements for completeness, accuracy, reliability and consistent intended performance (i.e. validation).
- b. Maintains SOPs for using these systems
- c. Ensure that the systems are designed to permit data changes in such a way that there is no deletion of entered data (i.e. maintain an audit trail, data trail, edit trail)
- d. Maintain a security system that prevents unauthorised access to the data
- e. Maintain a list of the individuals who are authorised to make data changes
- f. Maintain adequate backup of the data
- g. Safeguard the blinding, if any (e.g. maintain the blinding during data entry and processing)

4.2 Computerised Systems in Clinical Trials – 1999 Version

§XIII – System Dependability

C. Change Control

1. Written procedures should be in place to ensure that changes to the computerized system such as software upgrades, equipment or component replacement, or new instrumentation will maintain the integrity of the data or the integrity of protocols.
2. The impact of any change to the system should be evaluated and a decision made regarding the need to revalidate. Revalidation should be performed for changes that exceed operational limits or design specifications.
3. All changes to the system should be documented.

4.3 Computerised Systems in Clinical Trials – 2004 Version

§IX System Dependability

C. Change Control

FDA recommends that written procedures be put in place to ensure that changes to the computerized system, such as software upgrades, including security and performance patches, equipment, or component replacement, or new instrumentation, will maintain the integrity of the data and the integrity of protocols.

We recommend that the effects of any changes to the system be evaluated and a decision made regarding whether, and if so, what level of validation activities related to those changes would be appropriate.

We recommend that validation be performed for those types of changes that exceed previously established operational limits or design specifications.

Finally, we recommend that all changes to the system be documented.

(Expanded from the single paragraph in the original document).

4.4 Computerised Systems Validation in Clinical Research

Published by the Association for Clinical Data Management (ACDM – www.acdm.org.uk) this publication is in its 2nd Edition published in 2004; available as hardcopy for £30.

§12 Change Management

Change management is fundamental to the effective control and management of a system and therefore to its validated state. Change management ensures that each change introduced to the system (processes, people and technology) is appropriately defined, evaluated and approved prior to implementation. This evaluation ensures that the full implications and risks of any change are assessed against both the business and regulatory risks, including the level of cost and effort required.

§12.1 Change Control

It is necessary to control changes to a system in order to ensure that it continues to function as specified and is still fit for its intended purpose. Procedures should be in place to identify, authorise, validate, and implement changes to the system (technology, people and process).

These include changes made to:

- Hardware
- Software e.g. a specific application
- The environment in which it operates (e.g. operating system)
- The configuration of the hardware / software
- The use of the system (procedures)
- Roles and responsibilities
- Access control
- Training requirements
- Regulatory landscape
- The data and meta-data (unless addressed by audit trail functions and procedures)

Changes to a system may be requested either to correct an error or to reflect an enhancement or modification in functionality, access, performance or regulatory requirement. In all cases the reason for change should itself be clearly identified and documented. The following points should be considered:

- Requested changes should be documented in a register from which the status of all current and historical requests can be ascertained
- Risk assessment of the impact of the change (specifically against the user requirements and business processes)
- An impact assessment of the effect of a change on other parts of the system should be performed
- Approval for a change should be formally documented and sign-off by the system owner
- If approval is not given, the reason should be given
- Agreed changes to systems should be verified to ensure all requirements have been met
- The need for training should be assessed
- All related documentation should be updated e.g. SOPs, training material, requirements
- The change should be authorised and implemented, including delivery of any appropriate training.

It may also be necessary to allow provision for the development, testing and implementation of approved emergency changes in the production version of the system. An expedited version of the change management procedure should be in place for these very exceptional circumstances.

§12.2 Configuration Management

Configuration management is a discipline that establishes a system baseline and applies technical and administrative direction to the:

- Identification and documentation of the functional and physical characteristics of system components
- Controlled release of configuration changes
- Recording and reporting of the change control and implementation status
- Management of inter- and intra-system dependencies

§12.3 Version Control

Version control is essential for tracking all changes made to a system and associated documentation. This provides a complete history of the system and its various versions, as well as ensuring that the version of software and documentation in use at any given time can be uniquely identified and controlled (including specific versions of documents).

A unique identifier should be assigned to all system components and their related documentation.

Each new version, that is with new or changed functionality, should be distinguishable from its predecessors. Old versions of documents should be archived appropriately.

5 PIC/S Guidance: Computerised Systems in GXP Environments

5.1 §17. Change Management

17.1 It is important for proper control that a comprehensive change management system is instituted. This may take two forms in that during the Design phase it may only be necessary to keep records pertaining to the project up-to-date without formal “sign-off” approvals for all changes. However, once the project reaches a point where specifications are under development and conceptual aspects have been finalised, then a formal change control procedure should be established which will require clear, prescriptive and accurate documentation and records. It is important for the responsibilities of participants in the change control procedure to be carefully defined.

17.2 As discussed previously, it is appropriate for regulated users to have a *system control document* or some other record system to achieve a documented baseline record for the description of the computerised system. The system control documentation should be the definitive statement of what the system must do. The control document should also provide a record of the User Requirement Specifications. The change control procedure for the computerised system “project” should be integrated with the Master change control procedure for the regulated user organisation³⁰. *The change control procedure will need to take account of the corresponding procedures and records used by suppliers, integrators and other parties contracted to support the particular system and applications.* Validated decentralised arrangements for change control may be a feature in large complex regulated user companies.

³⁰ It is important for regulated users to ensure that change control management is in place during all system life cycle phases, i.e. from design and development through operation, maintenance, modification and retirement. The arrangements should be described in the validation plans for the project. Records should be kept with the project files.

17.3 Common IT infrastructure features may need to be controlled centrally by IT systems and security management. Key roles, responsibilities and procedures need to be clearly documented in relevant internal and external *Service Level Agreements*, (SLAs), or equivalent documents

5.2 §18. Change Control and Error Report System

18.1 The formal *change control procedure* should outline the necessary information and records for the following areas:

- *Records of details of proposed change(s) with reasoning.*
- *System status and controls impact prior to implementing change(s).*
- *Review and change authorisation methods (also see 12.5).*
- *Records of change reviews and sentencing (approval or rejection).*

- *Method of indicating 'change' status of documentation.*
- *Method(s) of assessing the full impact of change(s), including regression analysis and regression testing, as appropriate (IEEE).*
- *Interface of change control procedure with configuration management system.*

18.2 *The procedure should accommodate any changes that may come from enhancement of the system, i.e. a change to the user requirements specifications not identified at the start of the project. Or alternatively a change may be made in response to an error, deviation or problem identified during use of the system. The procedure should define the circumstances and the documentation requirements for emergency changes ("hot-fixes"). Each error and the authorised actions taken should be fully documented. The records should be either paper based or electronically filed.*

18.3 Computer systems seldom remain static in their development and use. For documentation and computer system control it should be recognised that there are several areas that would initiate change or a review for change. These are:

- a deviation report;
- an error report; or
- a request for enhancement of the computer system;
- hardware and software updates.

18.4 The results of periodic reviews may be helpful, e.g. in indicating process drifts and the need for change. *Quality systems procedures should ensure that the changes are clearly documented and closed out after actions have been completed. The change control procedure should complement and link with the deviation and errors report system. Various GAMP 4 'Operation' appendices include guidance in these areas.*

18.5 *The supplier of the software should have its own change control system in place and there should be clear and agreed procedures covering the interrelationship of the suppliers and users change control system. Where changes are made then the modifications of software should be undertaken following formal QMS documentation, records and procedural requirements.*

18.6 Any changes to the validated computerised system should not be undertaken without *review and authorisation* on behalf of all stakeholders responsible for the current user requirements. It may be appropriate for this to be undertaken by the system owner and QA representative. *Test scripts, determined by the project plan, q.v., (of defined test type and extent of tests), should be used to verify the acceptability of the software element developed in response to a change request. Integration testing may also be necessary before release of the new software version³¹.*

³¹ It may be necessary to regard proposed changes to infrastructure as a special case and define a set of stakeholders.

6 General Principles of Software Validation

6.1 §4.7. Software Validation after a Change

Due to the complexity of software, a seemingly small local change may have a significant global system impact. When any change (even a small change) is made to the software, the validation status of the software needs to be re-established. **Whenever software is changed, a validation analysis should be conducted not just for validation of the individual change, but also to determine the extent and impact of that change on the entire software system.** Based on this analysis, the software developer should then conduct an appropriate level of software regression testing to show that unchanged but vulnerable portions of the system have not been adversely affected. Design controls and appropriate regression testing provide the confidence that the software is validated after a software change.

Note, text in bold is in the original FDA document.

6.2 §5.2.7. Maintenance and Software Changes

As applied to software, the term maintenance does not mean the same as when applied to hardware. The operational maintenance of hardware and software are different because their failure/error mechanisms are different. Hardware maintenance typically includes preventive hardware maintenance actions, component replacement, and corrective changes. Software maintenance includes corrective, perfective, and adaptive maintenance but does not include preventive maintenance actions or software component replacement.

Changes made to correct errors and faults in the software are corrective maintenance. Changes made to the software to improve the performance, maintainability, or other attributes of the software system are perfective maintenance. Software changes to make the software system usable in a changed environment are adaptive maintenance.

When changes are made to a software system, either during initial development or during post release maintenance, sufficient regression analysis and testing should be conducted to demonstrate that portions of the software not involved in the change were not adversely impacted. This is in addition to testing that evaluates the correctness of the implemented change(s).

The specific validation effort necessary for each software change is determined by the type of change, the development products affected, and the impact of those products on the operation of the software. Careful and complete documentation of the design structure and interrelationships of various modules, interfaces, etc., can limit the validation effort needed when a change is made. The level of effort needed to fully validate a change is also dependent upon the degree to which validation of the original software was documented and archived. For example, test documentation, test cases, and results of previous verification and validation testing need to be archived if they are to be available for performing subsequent regression testing. Failure to archive this information for later use can significantly increase the level of effort and expense of revalidating the software after a change is made.

In addition to software verification and validation tasks that are part of the standard software development process, the following additional maintenance tasks should be addressed:

- **Software Validation Plan Revision** - For software that was previously validated, the existing software validation plan should be revised to support the validation of the revised software. If no previous software validation plan exists, such a plan should be established to support the validation of the revised software.

- **Anomaly Evaluation** – Software organizations frequently maintain documentation, such as software problem reports that describe software anomalies discovered and the specific corrective action taken to fix each anomaly. Too often, however, mistakes are repeated because software developers do not take the next step to determine the root causes of problems and make the process and procedural changes needed to avoid recurrence of the problem. Software anomalies should be evaluated in terms of their severity and their effects on system operation and safety, but they should also be treated as symptoms of process deficiencies in the quality system. A root cause analysis of anomalies can identify specific quality system deficiencies. 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. (See 21 CFR 820.100.)
- **Problem Identification and Resolution Tracking** - All problems discovered during maintenance of the software should be documented. The resolution of each problem should be tracked to ensure it is fixed, for historical reference, and for trending.
- **Proposed Change Assessment** - All proposed modifications, enhancements, or additions should be assessed to determine the effect each change would have on the system. This information should determine the extent to which verification and/or validation tasks need to be iterated.
- **Task Iteration** - For approved software changes, all necessary verification and validation tasks should be performed to ensure that planned changes are implemented correctly, all documentation is complete and up to date, and no unacceptable changes have occurred in software performance.
- **Documentation Updating** – Documentation should be carefully reviewed to determine which documents have been impacted by a change. All approved documents (e.g., specifications, test procedures, user manuals, etc.) that have been affected should be updated in accordance with configuration management procedures. Specifications should be updated before any maintenance and software changes are made.

7 NIST Special Publication 800-40 – Handling Security Patches

7.1 Executive Summary

Timely patching is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is the most common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches.

Vulnerabilities are weaknesses in software that can be exploited by a malicious entity to gain greater access and/or permission than it is authorized to have on a computer. Not all vulnerabilities have related patches; thus, system administrators must not only be aware of vulnerabilities and patches, but also mitigate “unpatched” vulnerabilities through other methods (e.g. workarounds, firewalls, and router access control lists).

To help address this growing problem, we recommend that organizations have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches. This document provides principles and methodologies for accomplishing this. One of several possible techniques is through the creation of a patch and vulnerability group (PVG). This group would facilitate the identification and distribution of patches within the organization. Its duties should include:

1. Creating an organizational hardware and software inventory
2. Identifying newly discovered vulnerabilities and security patches
3. Prioritizing patch application
4. Creating an organization-specific patch database
5. Testing patches for functionality and security (to the degree that resources allow)
6. Distributing patch and vulnerability information to local administrators
7. Verifying patch installation through network and host vulnerability scanning
8. Training system administrators in the use of vulnerability databases
9. Deploying patches automatically (when applicable)
10. Configure Automatic Update of Applications (when applicable).

If organizations use the PVG approach, this would not diminish the responsibility of all systems administrators to patch the systems under their control. Each systems administrator would:

1. Apply patches identified by the PVG
2. Test patches on the specific target systems
3. Identify patches and vulnerabilities associated with software not monitored by the PVG

Besides creating a PVG, organizations should be aware that applying patches and mitigating vulnerabilities is not always a straightforward process. To help with this, our document covers areas such as prioritizing patches, obtaining patches, testing patches, and applying patches.

7.2 Document Structure

The document is divided into six sections followed by seven appendices. The remainder of this document is structured as follows:

- Section 2 describes how to create and implement a patching policy, process, and system.
- Section 3 presents an overview of the various methods of identifying vulnerabilities and applicable patches.
- Section 4 gives an overview of specific government patch and vulnerability resources.
- Section 5 specifies patching procedures.
- Section 6 summarizes our recommendations for applying security patches.
- Appendix A presents a glossary of terms used throughout this document.
- Appendix B specifies patching resources for a variety of platforms and applications.
- Appendix C provides guidance on using the ICAT website to identify vulnerabilities and applicable patches.
- Appendix D identifies some commonly used vulnerability advisory resources.
- Appendix E details instructions for using the Windows Update feature included with most newer versions of Microsoft's Windows Operating System.
- Appendix F presents detailed instructions on using the Microsoft Baseline Security Advisor.
- Appendix G gives detailed instructions on downloading and using Microsoft's Network Security Hotfix Checker.
- Appendix H provides detailed instructions on downloading and using Microsoft's Qfecheck hotfix checker.

8 ISO 17799 Information Security Management

8.1 §8.1.2 Operational Change Control

Changes to information processing facilities and systems should be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures.

Operational programs should be subject to strict change control. When programs are changed, an audit log containing all relevant information should be retained. Changes to the operational environment can impact on applications. Wherever practicable, operational and application change control procedures should be integrated (see also 10.5.1). In particular, the following controls should be considered:

- a) identification and recording of significant changes;
- b) assessment of the potential impact of such changes;
- c) formal approval procedure for proposed changes;
- d) communication of change details to all relevant persons;
- e) procedures identifying responsibilities for aborting and recovering from unsuccessful changes.

8.2 §10.5 Security in Development and Support Processes

Objective: To maintain the security of application system software and information.
Project and support environments should be strictly controlled.

Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

§10.5.1 Change Control Procedures

In order to minimize the corruption of information systems, there should be strict control over the implementation of changes. Formal change control procedures should be enforced. They should ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. Changing application software can impact the operational environment. Wherever practicable, application and operational change control procedures should be integrated (see also 8.1.2). This process should include:

- a) maintaining a record of agreed authorization levels;
- b) ensuring changes are submitted by authorized users;
- c) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;
- d) identifying all computer software, information, database entities and hardware that require amendment;

- e) obtaining formal approval for detailed proposals before work commences;
- f) ensuring that the authorized user accepts changes prior to any implementation;
- g) ensuring that implementation is carried out to minimize business disruption;
- h) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;
- i) maintaining a version control for all software updates;
- j) maintaining an audit trail of all change requests;
- k) ensuring that operating documentation (see 8.1.1) and user procedures are changed as necessary to be appropriate;
- l) ensuring that the implementation of changes takes place at the right time and is not disturbing the business processes involved.

Many organizations maintain an environment in which users test new software and which is segregated from development and production environments. This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes.

§10.5.2 Technical Review of Operating System Changes

Periodically it is necessary to change the operating system, e.g. to install a newly supplied software release or patches. When changes occur, the application systems should be reviewed and tested to ensure that there is no adverse impact on operation or security. This process should cover:

- a) review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;
- b) ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;
- c) ensuring that notification of operating system changes is provided in time to allow appropriate reviews to take place before implementation;
- d) ensuring that appropriate changes are made to the business continuity plans (see clause 11).

§10.5.3 Restrictions on Changes to Software Packages

Modifications to software packages should be discouraged. As far as possible, and practicable, vendor-supplied software packages should be used without modification. Where it is deemed essential to modify a software package, the following points should be considered:

- a) the risk of built-in controls and integrity processes being compromised;
- b) whether the consent of the vendor should be obtained;
- c) the possibility of obtaining the required changes from the vendor as standard program updates;
- d) the impact if the organization becomes responsible for the future maintenance of the software as a result of changes.

If changes are deemed essential the original software should be retained and the changes applied to a clearly identified copy. All changes should be fully tested and documented, so that they can be reapplied if necessary to future software upgrades.

§10.5.4 Covert Channels and Trojan Code

A covert channel can expose information by some indirect and obscure means. It may be activated by changing a parameter accessible by both secure and insecure elements of a computing system, or by embedding information into a data stream. Trojan code is designed to affect a system in a way that is not authorized and not readily noticed and not required by the recipient or user of the program. Covert channels and Trojan code rarely occur by accident. Where covert channels or Trojan code are a concern, the following should be considered:

- a) buying programs only from a reputable source;
- b) buying programs in source code so the code may be verified;
- c) using evaluated products;
- d) inspecting all source code before operational use;
- e) controlling access to, and modification of, code once installed;
- f) use staff of proven trust to work on key systems.

§10.5.5 Outsourced Software Development

Where software development is outsourced, the following points should be considered:

- a) licensing arrangements, code ownership and intellectual property rights (see 12.1.2);
- b) certification of the quality and accuracy of the work carried out;
- c) escrow arrangements in the event of failure of the third party;
- d) rights of access for audit of the quality and accuracy of work done;
- e) contractual requirements for quality of code;
- f) testing before installation to detect Trojan code.

9 Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software

This guidance for industry was issued by the Center for Devices and Radiological Health in January 2005 and is reproduced in its entirety with the exception of the title pages and table of contents.

This guidance represents the Food and Drug Administration's (FDA's) current thinking on this topic. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. You can use an alternative approach if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach, contact the FDA staff responsible for implementing this guidance. If you cannot identify the appropriate FDA staff, call the appropriate number listed on the title page of this guidance.

9.1 Introduction

A growing number of medical devices are designed to be connected to computer networks. Many of these networked medical devices incorporate off-the-shelf software that is vulnerable to cybersecurity threats such as viruses and worms. These vulnerabilities may represent a risk to the safe and effective operation of networked medical devices and typically require an ongoing maintenance effort throughout the product life cycle to assure an adequate degree of protection. FDA is issuing this guidance to clarify how existing regulations, including the Quality System (QS) Regulation, apply to such cybersecurity maintenance activities. FDA's guidance documents, including this guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.

9.2 The Least Burdensome Approach

We believe we should consider the least burdensome approach in all areas of medical device regulation. This guidance reflects our careful review of the relevant scientific and legal requirements and what we believe is the least burdensome way for you to comply with those requirements. However, if you believe that an alternative approach would be less burdensome, please contact us so we can consider your point of view. You may send your written comments to the contact persons listed on the coversheet to this guidance or to the CDRH Ombudsman. Comprehensive information on CDRH's Ombudsman, including ways to contact him, can be found on the Internet at <http://www.fda.gov/cdrh/ombudsman/>.

9.3 Background

This guidance outlines general principles that we consider to be applicable to software maintenance actions required to address cybersecurity vulnerabilities for networked medical devices—specifically, those that incorporate off-the-shelf (OTS) software. The guidance is organized in question-and-answer format, providing responses to questions that have frequently been posed to FDA staff. The “I” in the questions and the “you” in the answers are intended to apply to device manufacturers who incorporate OTS software in their medical devices. The QS regulation, 21 CFR Part 820, applies to software maintenance actions. In addition, FDA has issued several guidance documents on software, including:

- General Principles of Software Validation; Final Guidance for Industry and FDA Staff, January 11, 2002, <http://www.fda.gov/cdrh/comp/guidance/938.html>.

- Guidance for Industry, FDA Reviewers and Compliance on Off-the-Shelf Software Use in Medical Devices, September 9, 1999, <http://www.fda.gov/cdrh/ode/guidance/585.html>.
- Guidance for FDA Reviewers and Industry, Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 29, 1998, <http://www.fda.gov/cdrh/ode/57.html>.

Questions and Answers

1. Which medical devices are covered by this guidance?

This guidance provides recommendations for medical devices that incorporate off-the-shelf (OTS) software and that can be connected to a private intranet or the public Internet. This guidance is addressed to device manufacturers who incorporate OTS software in their medical devices. However, this information also may be useful to network administrators in health care organizations and information technology vendors.

2. What is a cybersecurity vulnerability?

For purposes of this guidance, a cybersecurity vulnerability exists whenever the OTS software provides the opportunity for unauthorized access to the network or the medical device. Cybersecurity vulnerabilities open the door to unwanted software changes that may have an effect on the safety and effectiveness of the medical device.

3. What is it about “network-connected medical devices” that causes so much concern?

Vulnerabilities in cybersecurity may represent a risk to the safe and effective operation of networked medical devices using OTS software. Failure to properly address these vulnerabilities could result in an adverse effect on public health. A major concern with OTS software is the need for timely software patches to correct newly discovered vulnerabilities in the software.

4. Who is responsible for ensuring the safety and effectiveness of medical devices that incorporate OTS software?

You (the device manufacturer who uses OTS software in your medical device) bear the responsibility for the continued safe and effective performance of the medical device, including the performance of OTS software that is part of the device.¹

5. How should purchasers and users of these medical devices respond to information about a cybersecurity vulnerability?

FDA recommends that purchasers and users of medical devices that may be subject to a cybersecurity vulnerability contact you with their concerns. As Question 4 explains, you are responsible for the performance of OTS software that is part of your device. Although there may be times when it is appropriate for the user to become involved (see Question 9 below), the user should not attempt to make changes without seeking your advice and recommendations.

6. What regulations apply to software patches that address cybersecurity vulnerabilities?

The need to be vigilant and responsive to cybersecurity vulnerabilities is part of your obligation under 21 CFR 820.100 to systematically analyze sources of information and implement actions needed to correct and prevent problems. The preamble to the QS regulation explains that

actions taken should “be appropriate to the magnitude of the problem and commensurate with the risks encountered” (61 Fed. Reg. 52633; Oct. 7, 1996). Information in this guidance will remind you of some of the actions that ordinarily will be necessary to address this particular type of software concern.

Under 21 CFR 820.30(g), design validation requires that devices conform to defined user needs and intended uses, including an obligation to perform software validation and risk analysis, where appropriate. Software changes to address cybersecurity vulnerabilities are design changes and must be validated before approval and issuance. 21 CFR 820.30(i).

7. Is FDA premarket review required prior to implementation of a software patch to address a cybersecurity vulnerability?

Usually not. In general, FDA review is necessary when a change or modification could significantly affect the safety or effectiveness of the medical device. 21 CFR 807.81(a)(3), 814.39.

a. **510(k)**. For medical devices cleared for market under the 510(k) program, you may refer to our guidance entitled, “Deciding When to Submit a 510(k) for a Change to an Existing Device.”² That guidance explains that a new 510(k) submission to FDA is necessary for a change or modification to an existing medical device if:

- The medical device has a new or changed indication for use (e.g., the diseases or conditions the medical device is intended to treat); or
- The proposed change (e.g, modification in design, energy source, chemical composition, or material) could significantly affect the safety or effectiveness of the medical device.

It is possible, but unlikely, that a software patch will need a new 510(k) submission.³ As with all changes made to devices, you should document the basis of your decisions in the design history file. See 21 CFR 820.3(e), 820.30(j).

b. **Premarket Approval Application (PMA)**. For medical devices approved under PMAs (21 CFR Part 814), a PMA supplement is required for a software patch if the patch results in a change to the approved indications for use or is deemed by the manufacturer to have an adverse effect on the safety and effectiveness of the approved medical device. 21 CFR 814.39. Otherwise, you should report your decision to apply a software patch to your PMA device to FDA in your annual reports. See 21 CFR 814.39(b), 814.84.

8. Should I validate the software changes made to address cybersecurity vulnerabilities?

Yes. See answer to Question 4. You should validate all software design changes, including computer software changes to address cybersecurity vulnerabilities, according to an established protocol before approval and issuance. 21 CFR 820.30(i). You may refer to the “General Principles of Software Validation; Final Guidance for Industry and FDA Staff” (see **Background** section) for more information about how to validate software changes. For most software changes intended to address cybersecurity vulnerabilities, analysis, inspection, and testing should be adequate and clinical validation should not be necessary.

9. What else should I do to ensure cybersecurity for networked medical devices?

You should maintain formal business relationships with your OTS software vendors to ensure timely receipt of information concerning quality problems and recommended corrective and preventive actions. Because of the frequency of cybersecurity patches, we recommend that you develop a single cybersecurity maintenance plan to address compliance with the QS regulation and the issues discussed in this guidance document.

While it is customary for the medical device manufacturer to perform these software maintenance activities, there may be situations in which it is appropriate for the user facility, OTS vendor, or a third party to be involved. Your software maintenance plan should provide a mechanism for you to exercise overall responsibility while delegating specific tasks to other parties. The vast majority of healthcare organizations will lack detailed design information and

technical resources to assume primary maintenance responsibility for medical device software and, therefore, will rely on you to assume the primary maintenance responsibility.

10. Do I need to report a cybersecurity patch?

Not usually, because most software patches are installed to reduce the risk of developing a problem associated with a cybersecurity vulnerability and not to address a risk to health posed by the device. In most cases, therefore, you would not need to report a cybersecurity patch under 21 CFR Part 806 so long as you have evaluated the change and recorded the correction in your records. However, if the software patch affects the safety or effectiveness of the medical device, you should report the correction to FDA, even if a software maintenance plan is in effect.

¹ For more information, you should refer to “Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices,” Sept. 9, 1999 (see Background section of this guidance).

² “Deciding When to Submit a 510(k) for a Change to an Existing Device,” Jan. 10, 1997, <http://www.fda.gov/cdrh/ode/510kmod.html>.

³ If a submission is necessary, you should refer to “Guidance for FDA Reviewers and Industry, Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices,” May 29, 1998 (see Background section of this guidance).

Updated January 18, 2005