FDA Cybersecurity and Software Submission Guidance Update

Alan Kusinitz
www.softwarecpr.com
781-721-2921
alan@softwarecpr.com

SOFTWARE CPR
CRISIS PREVENTION AND RECOVERY, LLC

1

New FDA Guidance Documents

- Jan. 14, 2005 FDA guidance *Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*
- May 11, 2005 Direct to Final Revision of FDA's *Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices* .

2

FDA Contacts

- For questions regarding this document
- contact John F. Murray Jr. 240-276-0284, john.murray@fda.hhs.gov.
- David S. Buckles 301-443-8517 x174 david.buckles@fda.hhs.gov
- **Text on the following slides is from a presentation by John Murray, FDA CDRH Software and Part 11 Compliance Expert**

3

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.

4

Who is responsible for ensuring the safety and effectiveness of medical devices?

- The device manufacturer who uses OTS software in their medical device bears 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.
- The device manufacturer does not bear responsibility for the Hospital Network

5

Which medical devices are covered by this guidance?

Medical devices that incorporate off-the-shelf (OTS) software

- Medical Devices that can be connected to a private intranet or the public Internet
- Device manufacturers who incorporate OTS software in their medical devices.
- This information also may be useful to network administrators in health care organizations and information technology vendors.

6

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
- 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.

7

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
- **21 CFR 820.100** to systematically analyze sources of information and implement actions needed to correct and prevent problems.
- QS regulation preamble: actions taken should "be appropriate to the magnitude of the problem and commensurate with the risks encountered"
- **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).**

8

Is FDA premarket review required prior to implementation of a software patch ? - **Usually not**

- FDA review is necessary when a change or modification could significantly affect the safety or effectiveness of the medical device
- refer to our guidance entitled, "Deciding When to Submit a 510(k) for a Change to an Existing Device."
- It is possible, but unlikely, that a software patch will need a new 510(k) submission.
- 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).
- 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.

9

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

- Yes.
- 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)
- For most software changes intended to address **cybersecurity** vulnerabilities, analysis, inspection, and testing should be adequate and clinical validation should not be necessary.

10

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
- 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.

11

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.

12

The following are a few slides from

Brian Fitzgerald
Deputy Division Director,
Division of Software and Electronic Engineering,
Office of Science and Engineering Laboratories
12720 Twinbrook Pkwy HFZ-160
Rockville MD 20852-1720

brian.fitzgerald@fda.hhs.gov
(301) 443-2536 x140

Assistance is also available from the Division of Small Manufacturers, International and Consumer Assistance, http://www.fda.gov/cdrh/industry/support.
You don't have to be a manufacturer or consumer to avail yourself of their service!

This communication is consistent with 21 CFR 10.85(k) and constitutes an informal communication that represents my best judgment at this time but does not constitute an advisory opinion, does not necessarily represent the formal position of FDA, and does not bind or otherwise obligate or commit the agency to the view expressed.

13

What we know…

- Viruses in medical device software have already caused major disruptions to clinical information systems.
- Unspecified manufacturers have reportedly told hospital IT staff that they can't install security patches "because of FDA rules."

14

… and how we know it

- Very few formal complaints have been received from hospitals. Almost all our information is anecdotal.
- In some cases, clinical IT staff aren't plugged in to either the FDA or their own institution's biomedical engineering department.

Therefore be it resolved that

- FDA needs to do some outreach to the clinical IT community, and
- the biomedical engineering staff has to do the same within their hospital or clinical center.

15

Who actually owns the problem?

IT Infrastructure Vendors

Healthcare IT Administrators

Medical Device Manufacturers

16

FDA rules concerning design changes

- FDA requirements are aimed almost exclusively at the medical device manufacturer
- ***Not*** at the commercial off-the-shelf software vendor
- ***Not*** at the user or clinical facility

17

Essential elements of the plan

- Mechanism for timely notification of needed corrective actions from the COTS vendor.
- Competent evaluation of problem reports and patches, and documented decisions regarding corrective actions.
- Configuration management system in place for fielded systems for implementing patches.
- Technical support from the medical device manufacturer and/or COTS vendor available when needed.

18

SoftwareCPR Comments - Short term…

- Hold our breaths!
- Hope nothing bad happens.
- Make decisions based on public health risk (industry, FDA, and healthcare providers) – not just regulatory or legal.

19

SoftwareCPR Comments - Long Term…

- Risk Management in design of devices addresses this issue – isolates safety critical risk control measures from OTS/network attack
- OTS vendors provide more secure solutions
- Manufacturers and Healthcare providers accept responsibility and stop “assuming” networking is always acceptable.
- Different approaches depending on level of concern/risk?

20

May 11, 2005 Submission Guidance

- Direct to final... Not a significant change (except for BECS)
- Less verbose then the 1998 version
- Incorporates information on Special and Abbreviated 510(k)s
- Jointly issued by CDRH and CBER
- Addresses software information not all regulatory information in a submission – even if device is standalone software
- Off-the-shelf software information still addressed in separate guidance
- REMEMBER THERE ARE MANY DEVICE-SPECIFIC GUIDANCE

21

Terminology

- Clarifies that static analysis, code inspections, and reviews are a verification activity in addition to testing.
- Minor injury is any injury not meeting the 21 CFR 803 definition of serious injury
- Levels of Concern are stated in a revised manner

22

Levels of Concern (LOC)e

Indirect as well as direct effects should be considered

- Major – death or serious injury possible
- Moderate – minor injury possible
- Minor – **unlikely** to cause any injury (even if the failure occurs)
- Tables 1 and 2 provide a series of questions to determine software LOC.

23

Major and Moderate Level of Concern

1. Level of Concern
2. Software Description
3. Device Hazard Analysis
4. Software Requirements Specification
5. Architecture Design Chart
6. Software Design Specification
7. Traceability Analysis
8. Software Development Environment Description
9. Verification and Validation Documentation
10. Revision Level History
11. Unresolved Anomalies

24

Minor Level of Concern

1. Level of Concern
2. Software Description
3. Device Hazard Analysis
4. Summary of Functional Requirements from Software Requirements Specification
5. Traceability Analysis
6. Verification and Validation Documentation
7. Revision Level History

25

Software Description

- Comprehensive overview of the device features that are controlled by software, and describe operational environment
  - Paragraph format
  - Highlight major or operationally significant software features
  - Define programming language, hardware platform, operating system, OTSS
  - If information is in another document, can reference that document, e.g. SRS

26

Device Hazard Analysis

- Intended use hazards (foreseeable, intentional/inadvertent misuse of device
- Tabular form
- Line item for each identified hazard
- Each line should include (note no probability needed)
  - Identification of hazardous event
  - Severity of hazard
  - Cause(s) of hazard
  - Method of Control
  - Corrective measures taken,
  - Verification that method of control was implemented correctly

27

Software Requirements Specification (SRS)

- Hardware requirements and Programming Language Requirements including
  - Program size requirements/restrictions
  - Information on management of memory leaks
- Interface Requirements including communication between system components and with user: E.g., Printers, monitors, keyboard, mouse
- Performance and Functional Requirements
  - Algorithms or control characteristics
  - Limitations
  - Internal software tests and checks
  - Error and interrupt handling
  - Fault detection, tolerance, and recovery characteristics
  - Safety requirements
  - Timing and memory requirements
  - Identification of OTSS, if appropriate

28

Architecture Design Chart

- Flowchart or similar depiction of relationships among major functional units
- Include relationships to hardware and to data flows such as networking
- Detailed information such as state diagrams may be useful to clearly depict relationship among software functional units
- Can reference location if in another document such as SRS

29

Software Design Specification

- Information in the SDS should be sufficient to ensure that the work performed by the software engineers was clear and unambiguous, with minimal ad hoc design
- May contain references to other documents, e.g., detailed software specifications
- Adequate information to allow for review of implementation plan for requirements in terms of intended use, functionality, safety, and effectiveness
- Note key algorithms could be here or in SRS or elsewhere

30

Traceability Analysis

- Links requirements, design and testing
- Means of tying hazards with implementation and testing of mitigations
- Matrix with line items for requirements, specifications and tests, and pointers to hazard mitigations
- Can be a shared organizational structure with common numbering scheme
- Provide some mechanism, e.g., matrix, for guiding the reviewer

31

Software Development Environment Description

- Summary of software development life cycle plan
- For Major LOC also include annotated list of control/baseline documents generated during software development process and list or description of software coding standards
- Configuration Management and maintenance
  - For Moderate LOC a summary
  - For Major LOC ensure there is sufficient detail to allow a thorough understanding of configuration management and maintenance plan

32

Verification and Validation Documentation

- For Minor LOC – submit documentation of system or device level testing including pass/fail criteria and a summary of test results
- For Moderate and Major LOC submit
  - system level test protocol
  - summary list of validation and verification activities at unit, integration and system level and results of these activities and pass/fail criteria
  - ensure traceabilty analysis links these activities to requirements and specs
- For Major also submit
  - Description of any tests that were not passed and modifications in response to failed tests and evidence modifications were effective
  - Examples of unit and integaration testing and a summary of results.
  - Identify modifications made in response to failed tests and documentation that modifications were effective
  - Examples of unit, integration and system level testing and a summary of the results

33

Revision Level History

- History of software revisions generated during course of product development
- Line item tabulation of major changes to software during development cycle
  - Date
  - Version number
  - Brief description of changes
- Last entry should be final version to be released
  - Identify differences between tested version and released version along with assessment of potential effect of differences on safety and effectiveness

34

Unresolved Anomalies

- List of unresolved anomalies
  - Problem
  - Impact on device performance
  - Impact on safety and effectiveness, including operator usage and human factors
  - Plans and timeframes for correcting, when appropriate
  - Mitigations/workarounds
- Communicate to user

35

Abbreviated

- Declaration of Conformity to a standard
  - ISO/IEC 12207:1995
  - IEEE/EIA 12207.0-1996
  - AAMI / ANSI SW68:2001
  - UL 1998
- FDA recognition statements indicate what documentation can be omitted in the submission for each standard and level of concern.

36

Special 510(k)

- Submit documentation identified in guidance document but only for the modification that prompted the submission
  - The 510(k) paradigm guidance requires a comparison to the cleared device – does this mean more then just the change that triggered the 510(k) as stated above???
  - Submit test plans, pass/fail criteria, and summary results rather than test data
- Submit regression testing performed
- Risk analysis of changes

37

Additional Topics Section

- Risk Management
- Software Change Management
- Blood Establishment Computer Software (BECS)
- Software of Unknown Pedigree (SOUP)
- Virus Protection Software – **out of scope**
- Interfaces and Networking
- Combination Products

38

SoftwareCPR ®

- Provides software regulatory, validation, and safety news, examples, information and training aides via its website service at www.softwarecpr.com
- SoftwareCPR® also provides on-site and web-based training and consulting for medical device and pharmaceutical companies.
- Contact: Alan Kusinitz at alan@softwarecpr.com or 781-721-2921 for more information.

39