Guidance for Industry

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

Document issued on: January 14, 2005

For questions regarding this document contact John F. Murray Jr. 240-276-0284, john.murray@fda.hhs.gov. or David S. Buckles 301-443-8517 x174, david.buckles@fda.hhs.gov

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Compliance
Office of Device Evaluation

Preface

Public Comment

Written comments and suggestions may be submitted at any time for Agency consideration to the Division of Dockets Management, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD, 20852. When submitting comments, please refer to the exact title of this guidance document. Comments may not be acted upon by the Agency until the document is next revised or updated.

Additional Copies

Additional copies are available from the Internet at: http://www.fda.gov/cdrh/comp/guidance/1553.pdf. To receive this document by fax, call the CDRH Facts-On-Demand system at 800-899-0381 or 301-827-0111 from a touch-tone telephone. Press 1 to enter the system. At the second voice prompt, press 1 to order a document. Enter the document number (1553) followed by the pound sign (#). Follow the remaining voice prompts to complete your request.

Guidance for Industry

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

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.

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/.

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.

[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).

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).

---

[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).

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.