



U. S. Department of  
Health and Human Services



Center for Devices and  
Radiological Health

# FDA Regulatory Perspectives

Presented to ACCE and AAMI

Brian Fitzgerald

Deputy Division Director,

Division of Software and Electrical Engineering

Office of Science and Engineering Laboratories

Tampa, May 14-16, 2005

# Who am I?



Brian Fitzgerald  
Deputy Division Director,  
Division of Software and Electronic Engineering,  
Office of Science and Engineering Laboratories  
12720 Twinbrook Pkwy HFZ-141  
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.

# The burning question...



**Q.** Is FDA policy degrading network security and performance by impeding the timely implementation of security and other maintenance patches in commercial off-the-shelf (COTS) software used in network connected medical devices?

**A.** No. But there seems to be some confusion over what is required, and ***mistaken interpretations of FDA policy (and the law) may be contributing to the problem.***

# 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."

# ... 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.

# User facility reporting requirements



User facilities are required to report<sup>1</sup>:

- ◆ deaths involving medical devices to FDA and the manufacturer
- ◆ Serious injuries involving medical devices to the manufacturer, but not to FDA

Reporting is done via MedWatch  
([www.fda.gov/medwatch](http://www.fda.gov/medwatch))

Voluntary reports (when the user believes there is a potential for injury or death) can also be made to MedWatch.

<sup>1</sup> Food, Drug, and Cosmetic Act, §519(b)(1)

# Manufacturer reporting requirements



- ◆ Malfunctions that have caused or contributed to a death or serious injury, or are likely to cause or contribute to a death, must be reported to FDA<sup>1</sup>.
- ◆ Any indication of a quality deficiency must be investigated and resolved with the active participation of management.<sup>2</sup>

<sup>1</sup> Food, Drug, and Cosmetic Act, §519(a)(1), and §803/804 of regulations

<sup>2</sup> Quality System Regulation, §820.100

# Manufacturer reporting requirements (cont'd)

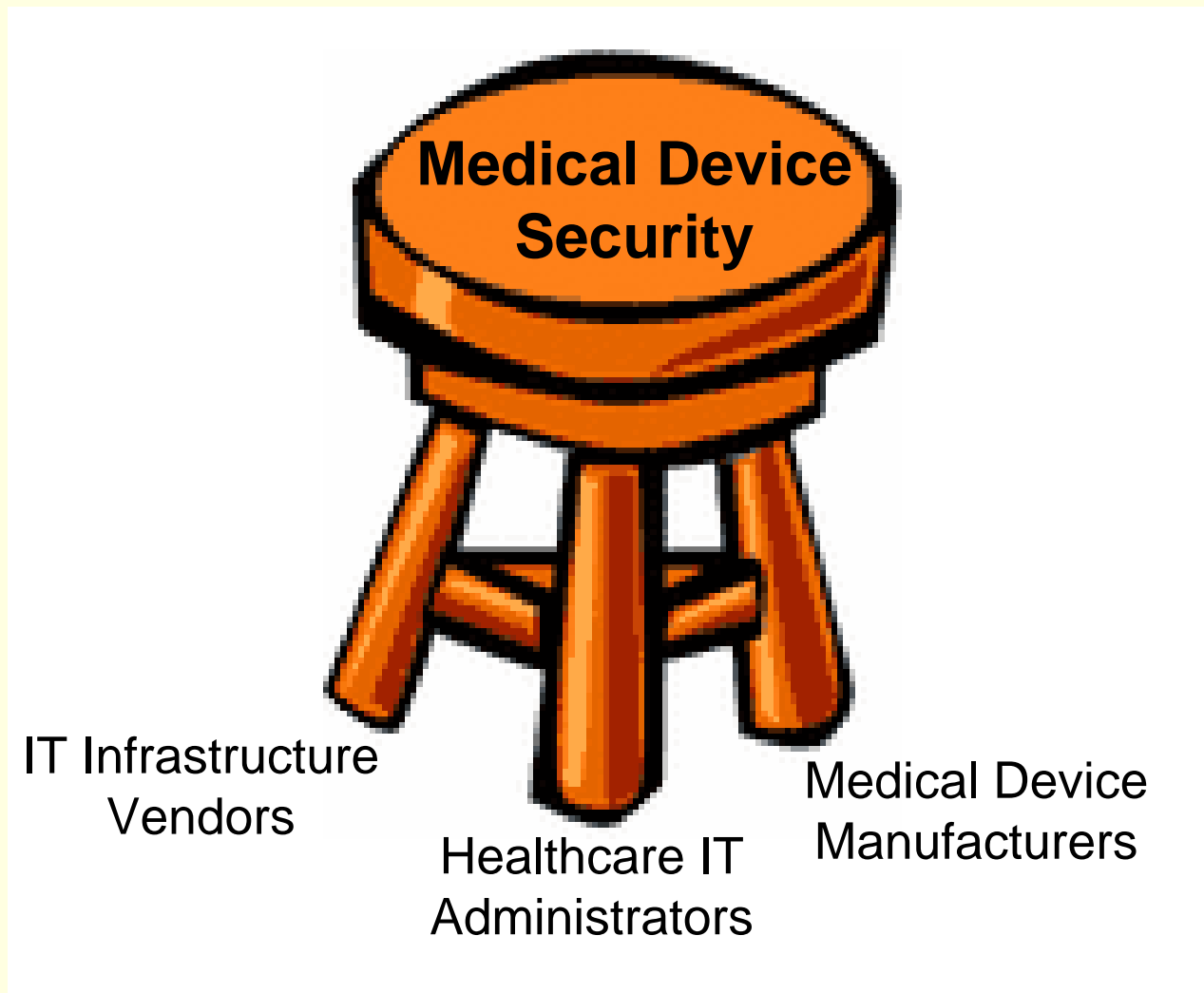
---



- ◆ Complaints must be evaluated in a timely manner, and investigated or reported to FDA as appropriate<sup>1</sup>.

<sup>1</sup> Quality System Regulation, §820.198

# Who actually owns the problem?



# 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

# What are the FDA rules applicable to software maintenance patches?

---



- ◆ Per the quality system regulation, 21 CFR 820.30(g), design changes must be validated by the manufacturer when the change cannot be verified by subsequent inspection and test.
- ◆ Per 21 CFR 807.81(a)(3), a change or modification in the device that could significantly affect the safety or effectiveness of the device requires a premarket notification by the manufacturer.

# Let's take those in reverse order...



A new premarket notification is needed if<sup>1</sup>:

- ◆ The proposed design change (i.e., the patch) affects the indications for use; or
- ◆ Clinical data are necessary to evaluate safety and effectiveness of the change, or
- ◆ Evaluation of the change raises new issues of safety and effectiveness.

***In other words, rarely.***

<sup>1</sup> CDRH Guidance Document, “Deciding When to Submit a 510(k) for a Change to an Existing Device,” Jan. 10, 1997

# Design changes must be verified and/or validated



This seems to be the sticking point for most.

- ◆ Proposed changes must be assessed in accordance with a documented change control process.
- ◆ Evaluations of proposed changes—i.e., decisions and their rationales—should be documented.
- ◆ People making decisions should be competent.

# A maintenance plan is the practical solution

- ◆ The manufacturer can fulfill their legal obligation by developing a maintenance plan for the COTS software in their device.
- ◆ The maintenance plan should be described in the premarket submission.
- ◆ The plan may delegate authority for carrying out aspects of the plan to some combination of
  - ◆ The user facility
  - ◆ The manufacturer
  - ◆ The COTS vendor
  - ◆ A third party
- ◆ Recurring cost of maintenance should be addressed.

# 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.

# In conclusion...

## For User facilities

- ◆ For networked devices ensure you have a maintenance plan from your device provider before you purchase.
- ◆ Rely on the device manufacturer for support, not on the COTS vendor.
- ◆ Use mandatory & voluntary reporting (MedWatch) to keep FDA informed.
- ◆ Complain in writing (or even verbally) to the device provider if malfunctions occur and prompt support is not forthcoming.
- ◆ Like it or not IT support professionals and Biomedical techs are joined at the hip!

## For COTS Vendors

- ◆ Provide transparency in your updates so your customers can tailor their updates to their customers.

## For Device manufacturers

- ◆ Provide details of your COTS maintenance plan during premarket submission