Considerations for using the Web for Medical Device Applications

MEDS, San Diego – August 23rd, 2012

Daniel Sterling, President
Who is Sterling?

Your Partner in Medical Device Development

What we do:

- System development and test
  - Software and Electronics Experts
  - Any Phase
- Risk planning and hazard identification
- DHF Remediation
- Project Rescue
- Quality System Consulting
- Host Management

300+ Projects with 100+ Clients

There when you need us!
Is Your App a Device? ... and if so??

In the United States

LAW (FD&C Act)

Regulation (21CFRxxx)

FDA Guidance

ANSI / AAMI / ISO / IEC Standards
Medical Device Defined

Section 201(h) of the FD&C Act:

“…an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent…..”, that is “...intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man...” or “...intended to affect the structure or any function of the body of man or other animals...”
Intended Use

21 CFR 801.4:

... may, for example, be shown by labeling claims, advertising matter, or oral or written statements by such persons or their representatives.

... by the circumstances that the article is, with the knowledge of such persons or their representatives, offered and used for a purpose for which it is neither labeled nor advertised.
What if my App is a Device?

- Impacts Design/Development
- Impacts Maintenance
Impact on Design/Development

Risk

Assess, Mitigate, Test & Trace

... and Repeat

How Much ➔ Determined by Class and LOC
Impact on Maintenance

- **Active Surveillance Program**
  - Relationship with vendor(s)
  - Gather field/use information

- **Configuration Control**

- **Update/Validate** – likely frequent
FDA Guidance for **Networked** Medical Applications:

Guidance for Industry, Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, January 14, 2005


→ Risk considerations for networked devices – vulnerable to altered behavior
→ Plan for control of the “device”, updates/patches
  → Drives requirements for client/mobile devices (e.g. control of OS updates)
  → Drives requirements for web services, including database maintenance
→ Subject to Validation – Design, not usually Clinical
→ Not usually subject to resubmission
  → When no impact on indication, efficacy and safety
## Impact of 62304

### Risk Management: SFMEA $\rightarrow$ Risk of Each Item/Unit

<table>
<thead>
<tr>
<th>ID</th>
<th>Class</th>
<th>Unit</th>
<th>Class</th>
<th>Sub-Unit</th>
<th>Class</th>
<th>Sub-Unit 2</th>
<th>Class</th>
<th>Potential Failure Mode</th>
<th>Potential Cause(s)/Mechanism(s) of Failure</th>
<th>Potential Effect(s) of Failure (Harm)</th>
<th>Sev</th>
<th>P1</th>
<th>P2</th>
<th>Risk</th>
<th>SRS ID</th>
<th>Mitigations</th>
<th>Res. Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Why P1 and P2??
Impact

Risk of Harm vs. Risk of Hazardous Situation

IEC 62304 says $P_1 = 1$
Types of Potential Risks & Causes Unique to Web/Networked Systems:

Safety/Efficacy Related:
   Altered Behavior
      → Browser/Server Hijacked
      → Packets Intercepted/Altered

Use Related
   → Delays lead to misuse
   → Lost packets cause errors in judgment

Privacy (HIPPA)
   → Packets Intercepted
   → Phishing

Theft (Intellectual Property)
   → Code transferred to client for execution, especially script
   → Packet Interception
Types of Potential Causes Unique to Web/Networked Systems:

How Can This Happen?

Exploit of vulnerabilities

→ SQL Queries Injected at the Client, Sent Through to Server
→ User Spoof – Create an admin account in application and/or database
→ Substitute Code at Client, Web Server, or Database (stored procedures)

Resources Unavailable

→ Transport Delays lead to user impatience
→ Resource availability and response hampered by competing services
  • Client or Server


Types of Potential Mitigations Unique to Web/Networked Systems:

How Can We Protect Ourselves?

Design

→ Prevent injection points in application UI
  → Don’t pass inputs through to server w/o validation
→ Actively Manage User Sessions
  → Session Handshaking
  → Message sequencing – for security and to prevent use errors
  → Client Monitor for Server Inconsistency
  → Server Monitor for Client inconsistency
  → Alarms
→ Use OTS/SOUP with lower probability of exploit (server enforced)
  → Secure browser through configuration
  → Use embedded browser
  → Use NO browser (e.g. Silverlight Client)
  → Avoid IE if possible, otherwise you need a vigorous maintenance program
→ Execute Business Logic (IP) on Server, when possible
  → “Rich” interfaces may need to run on client for responsiveness (e.g. a configurable graph)
  → Execute on client using binaries rather than script (e.g. library or control rather than Javascript)
→ Encrypt
  → Client/Server Communications
  → Databases
Types of Potential Mitigations Unique to Web/Networked Systems:

How Can We Protect Ourselves?

Design

→ Prevent/Minimize Competing Processes
  → On Client, run stand-alone (if possible)
  → On Client, monitor performance and alarm
  → On Server, host only your application (can’t use most commercial hosting providers)

→ Use Redundant Application and Database Servers
  → Monitor performance
  → Manage usage
  → Alarm
  → Partition Database Servers for Performance and Scalability

→ CRC Code
  → Periodically Monitor
  → Alarm

→ Network/Server Security – Lock it down!
  → Disable all unused ports
  → Avoid commonly used ports, if possible
Types of Potential Mitigations Unique to Web/Networked Systems:

How Can We Protect Ourselves?

Maintenance

→ Configuration Control Consistent with QRS/GMP/ISO13485
→ Expeditiously Patch all OTS/SOUP, Client and Server
→ Virus and Malware Surveillance
→ Audit User Accounts and Database Periodically (Script or Manual)
  → Look for unauthorized accounts
  → Look for data that is inconsistent with the application’s use of the database
→ Periodic Performance Testing
  → Degraded performance may indicate a compromised system
→ Periodic Network Validation
  → Services Running
  → Ports Open
  → User Accounts
Underlying FDA Guidance for Software:

• Guidance for Industry and FDA Staff -- Guidance for the Content of Premarket Submissions for Software Contained in Medical Device, May 11, 2005
  

→ What Documents to Submit to FDA

→ Based on Level of Concern

• General Principles of Software Validation; Final Guidance for Industry and FDA Staff, January 11, 2002
  

→ Name is deceiving; outlines “good content” for all/most design output

→ “Validation” is based on a preponderance of evidence that good practices were used.
Underlying FDA Guidance for Software:

Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Device, September 9, 1999

http://www.fda.gov/cdrh/ode/guidance/585.html

→ Defines OTS Software
→ What you need to do with OTS as part of Validation and Risk Assessment
A word about...

Medical Device Data Systems (MDDS)

New rule: 21 CFR 880.6310 (not just guidance)

The Good:

Reclassification from III to I

The Bad:

Makes it clear that more devices and organizations fall under Class I regulations

(e.g. hospitals developing/modifying their own systems which meet the definition)
FDA Guidance for Mobile Medical Applications:

Draft Guidance for Industry and Food and Drug Administration Staff, Mobile Medical Applications, DRAFT GUIDANCE, July 21, 2011


→ IMHO, nice summary - not much new, Just Another Computing Platform
→ Why? Because all the previous guidance covers mobile
→ Some clarification on types of apps which have not usually been considered devices (e.g. office automation, EMR accessories)
→ Distinguishes between manufacturers and distributors (e.g. iTunes)
→ If the intended use makes the mobile device into a medical device or a medical device accessory, then it is a medical device.
References

Standards:


• EN/ISO 14971:2009, Medical Devices – Application of Risk Management to Medical Devices

• IEC/EN 60601-1-4, Medical electrical equipment — Part 1-4: General requirements for safety — Collateral standard: Programmable electrical medical systems (absorbed into 60601-1, ch 14 in latest version)

Considerations for using the Web for Medical Device Applications

Daniel Sterling
President
Sterling Medical Devices
201-227-7569 x111
dan@sterlingmedicaldevices.com
www.sterlingmedicaldevices.com