Agenda

Day 1 ● Tuesday, April 14, 2015

8:00 a.m. – 8:30 a.m. **Registration and Continental Breakfast**

8:30 a.m. – 9:00 a.m. **Welcome and Introductions**

9:00 a.m. – 10:00 a.m.

I. **FDA's Research on Medical Device Software Best Practices**

II. **FDA's Analysis of Software-Related Recalls**

10:00 a.m. – 11:00 a.m.

III. **Overview of Recent FDA Guidances**

a. Cybersecurity in Medical Devices (draft, June 2013)
b. Radio Frequency Wireless Technology in Medical Devices (August 2013)
c. Mobile Medical Applications (September 2013)
d. Total Product Life Cycle: Infusion Pump (draft, April 2010)

11:00 a.m. – 11:15 a.m. **Refreshment Break**

11:15 a.m. – 12:15 p.m.

IV. **Key Relevant Standards**

a. ISO 14971:2007 and EN ISO 14971:2012, IEC TR 80002-1 Application of ISO 14971 for Software
b. IEC 62304 Medical Device Software Life Cycle Process - Risk Management Section
c. IEC 80001-1 Managing Medical IT-Networks and relevant Technical Reports
d. NIST Framework for Improving Critical Infrastructure Cybersecurity, 2014

12:15 p.m. – 12:45 p.m. **Morning Summary of FDA Perspectives and Group Discussion**

12:45 p.m. – 1:45 p.m. **Lunch**

1:45 p.m. – 2:45 p.m.

V. **Risk Management Documentation to Support Regulatory Filings and Inspections**

a. What is viewed as best practices to demonstrate safety

VI. **Risk Management Documentation for Pre-market Submissions**

a. **Case study for risk traceability matrix.** This study provides participants a template for and examples of best practices that are frequently requested for pre-market submissions or during establishment inspections

b. **Case study for cybersecurity risk traceability matrix.** This study provides participants a template for and examples of best practices that are frequently requested for pre-market submissions or during establishment inspections

2:45 p.m. – 3:00 p.m. **Refreshment Break**

3:00 p.m. – 4:30 p.m. VII. **Risk Management Completeness, Adequacy, Effectiveness and Reviewability**

a. Introduction of assurance case concepts and how they are used in industry
b. **Case study for medical device safety assurance case.** This study illustrates how to document information in a story telling fashion and convince internal/external reviewers (e.g. ODE reviewers) that a risk analysis is adequate and complete
c. **Case study for medical device cybersecurity assurance case.** This case study illustrates how to document information in a story telling fashion and convince internal/external reviewers (e.g. ODE reviewers) that a cybersecurity risk analysis is adequate and complete.

4:30 p.m. – 5:00 p.m. **Day One Summary of FDA Perspectives and Group Discussion**

Day 1 ● Wednesday, April 15, 2015

8:00 a.m. – 8:30 a.m. **Continental Breakfast**

8:30 a.m. – 9:00 a.m. VIII. **Characteristics for Medical Device Software**

a. Understanding the difference between software and hardware
b. Understanding software quality and reliability engineering
c. Challenges of software risk management and cybersecurity

9:00 a.m. – 9:30 a.m. IX. **Emerging Methods and Techniques**

a. Learn what new technical methods and techniques the FDA has been researching and looking into to improve the safety of software related medical devices

9:30 a.m. – 10:30 a.m. X. **Risk Identification**

a. Preliminary hazard analysis
b. Top down analysis, fault tree analysis
c. Bottom up analysis – including design FMEA, function FMEA, process FMEA, usability FMEA, common causes of software failures
d. Connectivity analysis between top down and bottom up
e. Multi perspective analysis
f. **Case study.** This study provides participants an opportunity to apply techniques on how to identify and connect hazards, hazardous situations/causes using device examples.

10:30 a.m. – 10:45 a.m. **Refreshment Break**

10:45 a.m. – 11:45 a.m. XI. **Cybersecurity Risk Identification**

a. Medical device cybersecurity basics
b. Asset profiling
c. Threat identification
d. Vulnerability identification
e. Software vulnerabilities
f. Connectivity between cybersecurity and safety risk analysis
g. **Case study.** This study provides participants an opportunity to apply techniques on how to identify and connect assets, threats and vulnerabilities using device examples.

11:45 a.m. – 12:15 p.m. Morning Summary of FDA Perspectives and Group Discussion

12:15 p.m. – 1:15 p.m. Lunch

1:15 p.m. – 2:15 p.m. XII. **Risk Controls**

a. Risk control basics
b. Software life cycle process control measures
c. Safety requirements identification
d. Cybersecurity capability and requirements identification
e. Special considerations for cybersecurity risk controls
f. Control measures implementation and effectiveness
g. **Case study.** This study provides participants an opportunity to identify, apply risk controls and establish traceability of its implementation using device examples.

2:15 p.m. – 3:15 p.m. XIII. **Software-Related Medical Device Risk Assessment and Evaluation**

a. Pre-market risk assessment and evaluation
b. Post-market risk assessment and evaluation
c. Legacy product cybersecurity risk management
d. Maintenance and life cycle risk management

3:15 p.m. – 3:45 p.m. XIV. **Success Factors for Risk Management Programs**

3:45 p.m. – 4:15 p.m. **Day Two Summary of FDA Perspectives and Group Discussion Plus Workshop Wrap Up**