Regulatory and Compliance Assessment of Connected Medical Devices – Status and Discussion

Dr. Sarbari Gupta

President and CEO, Electrosoft

International Risk Governance Council (IRGC) Workshop on

Governing Cyber Security Risks and Benefits in the Internet of Things

Swiss Re Center for Global Dialogue, Zurich

November 15-16, 2016

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
FAX: (703) 437-9452

Agenda

- **Background**
  - ***Overview of Security Challenges and Risks***
  - ***Status of Relevant Standards and Compliance Programs***
- **Discussion**
  - ***What Exists? What's Needed?***
  - ***Core Cybersecurity Principles***
  - ***Evaluation and Assessment Models***

Connected Medical Devices – Security Challenges and Risks

- **Cybersecurity Challenges**
  - ***Unauthorized Access to PII (incl. Health Data)***
  - ***Unauthorized Modification of Therapy / Patient Data***
  - ***Loss of Connectivity***
  - ***Potential Launch Point for Attacks on Health Network***
- **Constraints**
  - ***Physical Location of Device (in Operational Mode)***
  - ***Computational Capacity***
  - ***Battery Power***
  - ***Storage Capacity***
  - ***Limited Connectivity Options (Wi-fi, Bluetooth)***
- **Need for Regulation and Compliance**
  - ***Patient Health Risk***
  - ***Patient Privacy Risk***
  - ***Provider Network Risk***

FDA Guidance – OTS Software – Jan 2005

- **Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software**
  - ***Vendors responsible to ensure OTS software is secure and is patched when needed for safety of device***
  - ***Purchasers and Users may contact Vendor regarding vulnerability***
  - ***Software changes to address cybersecurity vulnerabilities must be validated before approval (21 CFR 820.30(i))***
  - ***FDA Premarket review generally not required for software patches addressing cybersecurity vulnerabilities***
  - ***Cybersecurity patches need not be reported unless they impact the safety or effectiveness of the medical device***

FDA Guidance – Pre-Market Submissions – Oct 2014

- **Content of Premarket Submissions for Management of Cybersecurity in Medical Devices**
  - ***General Principles***
    - **Identify Assets/Threats/Vulnerabilities**
    - **Assess Impact of Threats and Vulnerabilities**
    - **Determine Likelihood of Occurrence**
    - **Determine Risk Levels**
    - **Assess Residual Risk and Acceptance Criteria**
  - ***Cybersecurity Functions***
    - **Identify and Protect**
      - *Limit Access to Trusted Users Only*
      - *Ensure Trusted Content*
    - **Detect, Respond and Recover**
      - *Implement mechanisms to detect compromise*
      - *Involve Patient upon cyber event*
      - *Protect Critical Functionality*
      - *Retain and recover configurations by privileged user*

FDA Draft Guidance – Post-Market Management – Jan 2016

- **Post-Market Management of Cybersecurity of Medical Devices**
- **Cybersecurity is a shared responsibility**
  - ***Patients, providers, manufacturers and healthcare facilities***
- **Cybersecurity compromise can impact:**
  - ***Device functionality; Data Loss (medical or personal); Availability; Integrity and Other connected devices***
- **Elements of Effective Postmarket Cybersecurity Program**
  - ***Identify***
    - **Define Essential Clinical Performance**
    - **Identification of Cybersecurity Signals**
  - ***Protect/Detect***
    - **Vulnerability Characterization and Assessment**
    - **Risk Analysis and Threat Modeling**
    - **Analysis of Threat Sources**
    - **Threat Detection Capabilities**
    - **Impact Assessment on all Devices (for manufacturer)**
  - ***Detect/Respond/Recover***
    - **Compensating Controls Assessment**
    - **Risk Mitigation of Essential Clinical Performance**

DTSec – Diabetes Medical Device Standard – May 2016

- **Standard for Wireless Diabetes Device Security (DTSec)**
- **Leverages ISO 15408 – Common Criteria**
  - ***Protection Profiles (PP) - generalize the requirements for a class of similar devices***
  - ***Security Targets (ST) – provide specific requirements for a specific product from a specific manufacturer***
- **General Principles**
  - ***Identification of assets, threats, and vulnerabilities***
  - ***Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients***
  - ***Assessment of the likelihood of a threat and of a vulnerability being exploited***
  - ***Determination of risk levels and suitable mitigation strategies***
  - ***Assessment of residual risk and risk acceptance criteria***
- **Assurance Program**
  - ***Lab Accreditation***
  - ***Product Certification***
  - ***Evaluated Products List***
  - ***PP and ST Approval***
  - ***Assurance Maintenance Program***
- **Structure and Concept applicable to other medical devices**

Other Relevant Standards/Guidelines

- **ISO IEC 62304 – Medical Device Software – Software Life Cycle Process**
- **IEC 82304-1:2016 – Applies to the safety and security of health software products designed to operate on general computing platforms**
- **ISO/DIS 27799 – Health Informatics – Information Security Management in Health using ISO/IEC 27002**
- **ISO 13485:2016 – Medical devices -- Quality management systems -- Requirements for regulatory purposes**
- **AAMI TIR57 – Principles for Medical Device Security – Risk Management**
- **HITRUST Common Security Framework (CSF)**

Agenda

- **Background**
  - ***Overview of Security Challenges and Risks***
  - ***Status of Relevant Standards and Compliance Programs***

- **Discussion**
  - ***What Exists? What's Needed?***
  - ***Core Cybersecurity Principles***
  - ***Evaluation and Assessment Models***

What Exists Today?

- **Guidance/Standards for**
  - ***Software Development Practices***
  - ***Patching of OTS Software***
- **Guidance on Risk Management Models**
- **Guidance on Pre-Market Submissions and Post-Market Management**
- **Definition of Common Criteria based Assurance Program (for diabetes control devices)**

What's Missing / Needed?

- **Cybersecurity Architecture Framework**
  - ***For use by Connected Medical Device Vendors and Evaluators***
  - ***Core Cybersecurity Principles***
  - ***Worksheets/Models that enable good design choices***
  - ***Documentation templates that enable effective articulation and evaluation of device cybersecurity architecture***
- **Cost-effective Models for Evaluation of Cybersecurity**
  - ***Who Evaluates?***
  - ***How Much Rigor?***
  - ***Evaluated Status Maintenance?***

Connected Medical Device - Cybersecurity Principles (I)

- **Unique Device ID**
  - ***Assign GUID for each Device – impossible to guess***
- **Manage Data:**
  - ***Minimize PII on Device***
  - ***Maintain Audit Records***
- **Limit Access**
  - ***Identify and Authenticate***
  - ***Establish Roles, Need to Access, Privileges***
  - ***Emergency Access***
- **Secure Communication Channels**
  - ***Minimize Content Pushed out***
  - ***Secure Communication Channels***

Connected Medical Device - Cybersecurity Principles (II)

- **Therapy Configuration (if applicable)**
  - ***Validate External Commands***
  - ***Validate Therapy Updates***
    - **2-Person Rule for Therapy Updates**
    - **Proximity Rule for Therapy Updates**
- **Alerts**
  - ***Patient Alerts on Significant Events***
- **Software Updates**
  - ***Authenticated Content***
  - ***Patient Consent/Involvement***

Evaluation & Assessment Models (I)

- ***What:*** **Methods to develop confidence that a product, service or system:**
  - ***Meets specified requirements***
  - ***Demonstrates required characteristics***
  - ***Performs in a specified manner***
- ***How:*** **Assessment rigor/formality can vary:**
  - ***Self-Assertions by Supplier***
  - ***Inspections based on Professional Judgment***
  - ***Testing using Technical Operations, Procedures***
  - ***Certification by Third Parties***

Evaluation & Assessment Models (II)

- ***Who:* Assessment can be performed by:**
  - ***Supplier – <u>First-Party</u>***
  - ***Consumer/Purchaser – <u>Second-Party</u>***
  - ***Independent Party hired by Supplier or Consumer – <u>Third-Party</u>***
  - ***Regulatory Body – <u>Third-Party</u>***
- ***When:* Assessment timing can be:**
  - ***One Time – Prior to Acquisition/Use***
  - ***Periodic – Established Interval***
  - ***Ad Hoc – As-Needed during Period of Use to Maintain Assurance***

Contact & Company Information

- **Contact Info: Dr. Sarbari Gupta – Electrosoft**
  - ***Email: sarbari@electrosoft-inc.com; Phone: 703-437-9451 ext 12***
  - ***LinkedIn: http://www.linkedin.com/profile/view?id=8759633***
- **About Electrosoft**
  - ***We deliver a diversified set of technology-based solutions and services with a deep focus on cybersecurity***
  - ***We co-authored over a dozen NIST security publications!***
  - ***Major Customers: DoD, GSA, Treasury, VA, DHS***
  - ***Founded in 2001; Headquartered in Reston, Virginia***
  - ***Socio-economic Certifications: 8(a), SDB, EDWOSB***
  - ***ISO 9001:2008 registered; CMMI Level 3 for DEV and SVC***
  - ***Website: http://www.electrosoft-inc.com***
- **What Makes Us Different?**
  - ***Cybersecurity is in our DNA! –*** *We inject a cybersecurity risk management/compliance dimension to every effort we undertake*
  - ***Our Core Values guide our every action!*** *– Our six core values of Integrity, Customer Service, Excellence, Teamwork, Accountability and Respect are evident through our attitude and our work*