Mobile Medical Applications …from the trenches

Peggy McLaughlin
MPM Advisors
MPMAdvisors@gmail.com

Apps by the Numbers

- The Apple & Google stores each have over 1,000,000 iPhone and Android Apps respectively.

- 1.5% of these apps are Mobile Medical Apps (MMA).

Apple ~ 2%

Google ~ 1%

MMA = regulatory oversight

Is your App a MMA?

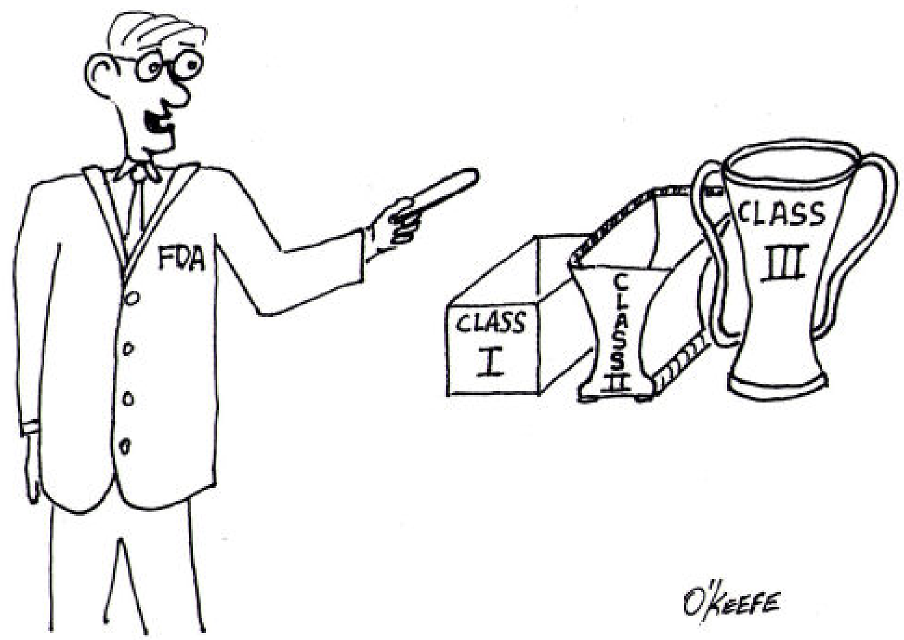
What is your intended use?

OR....

Is your App a MMA?

…and then how would it be classified?

Consider the risk…



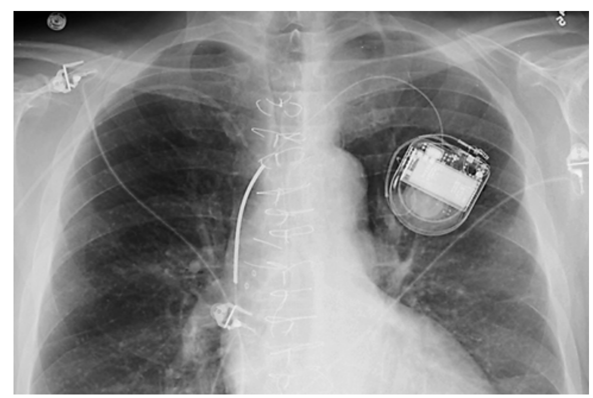
Eenie, meenie, mynie, moe, in which bin should the tongue depressor go?

FDA Classification

Class I (Low Risk)
–Generally not requiring a 510(k) notification

Class II (Medium Risk)
–Generally requiring a 510(k) notification

Class III (High Risk)
–Require Premarket Approval (PMA)



Regulatory 101

- Establishment registration, and Medical Device listing (21 CFR Part 807);
- Quality System (QS) regulation (21 CFR Part 820);
- Labeling requirements (21 CFR Part 801);
- Medical Device Reporting (21 CFR Part 803);
- Premarket notification (21 CFR Part 807);
- Reporting Corrections and Removals (21 CFR Part 806);
- Investigational Device Exemption (IDE) requirements for clinical studies of investigational devices (21 CFR Part 812).

Mobile Medical Apps

- AirStrip RPM by Airstrip Technologies

  Remote ECG monitor

- Triton System by Gauss Surgical

  Sponge counter & EBL estimation

Take home #1

It’s software!

Establish the ‘Level of Concern’

Use those FDA Guidance documents:

- 1999 Off the shelf (OTS) software
- 2002 Software Validation
- 2005 Cybersecurity …OTS
- 2005 Contents for submission…software

More Guidance

- 2011 Human Factors
- 2013 Mobile Medical Applications
- 2013 RF Wireless (draft)
- 2014 Contents of submission…cybersecurity

Take Home #2

software…with cybersecurity issues

→ Use your risk management process

See new Guidance document

- require secure authentication for access
- use encryption
- ensure security patches are added when necessary

Cybersecurity

…aspects of your device vis-à-vis information security:

- Confidentiality - no unauthorized users have access to the information.
- Integrity - the information is correct - that is, it has not been improperly modified.
- Availability - the information will be available when needed.
- Accountability - identification and authentication to assure that the prescribed access process is being done by an authorized user.

Take Home #3

Verification & Validation Testing

- Provide a rationale for a clinically relevant acceptance criteria.
- Test compared to a valid scientific method
- Consider pilot testing
- Training and testing sets must remain separate
- Consider ‘stand alone’ versus live clinical testing.

Take Home #4

Consider Electromagnetic Compatibility Issues

> '*introduction of radiated energy into the operating environment raises issues regarding EMC, wireless coexistence, wireless performance and data integrity, and wireless data security.*'

EMC

Address potential adverse interactions with wireless connections (Wi-Fi, Bluetooth, etc.), cellular connections, and other software applications with your testing.

EMC

- Validation in the intended use environment.
  - Wireless coexistence
  - Performance: Data latency & throughput
  - Performance: Limitations or restrictions for proper device operation or wireless communications
  - Data integrity
  - Security: Protections against unauthorized access to device control
  - Security: Protections against unauthorized access to data
  - EMC: Electromagnetic Interference - device responses / failures
- 60601-1-2 Testing (!?!)

Take Home #5

Software distribution methods:

- Consider your plans early on.
- Who will control distribution?
- How will upgrades be released?
- How will upgrades be distributed?
- What about upgrades to OTS?

Other kernels…

- FDA is concerned that physicians will OVERESTIMATE the accuracy of digitally provided information

  → Consider appropriate labeling which mitigates that concern
- FDA may want verification data in machine readable format

Other Regulations

- Federal Trade Commission (FTC)
- Federal Communications Commission (FCC)
- Health Insurance Portability and Accountability Act (HIPAA)

ISO Standards

- ISO/IEC 90003:2004, *Software engineering -- Guidelines for the application of ISO 9001:2000 to computer software*, 2004.
- ISO 14971:2007, Medical Devices - Risk Management - Part 1: Application of Risk Analysis, 2007.
- IEC 62304:2006, *Medical device software – Software life cycle processes*, 2006.
- IEEE Std 1012-2004, *IEEE Standard for Software Verification and Validation*, 2004.

ISO Standards

- *IEEE Standards Collection, Software Engineering*, 1994. ISBN 1-55937-442-X.
- ISO/IEC 25051:2006, *Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing*, 2006.

ISO Standards

- ISO/IEC 12207:2008, *Systems and software engineering – Software life cycle processes, 2008* and IEEE Std 12207-2008, *Systems and software engineering – Software life cycle processes, 2008.*
- ISO/IEC 14598:1999, *Information technology - Software product evaluation*, 1999.
- AAMI TIR32:2004, *Medical device software risk management*, 2004.
- AAMI TIR36:2007, *Validation of software for regulated processes*, 2007.

ISO Standards

- ANSI/AAMI/IEC TIR80002-1:2009, Medical device software - Part 1: *Guidance on the application of ISO 14971 to medical device software*, 2009. (Identical adoption of IEC/TR 80002-1:2009)
- *Clause 14* of IEC 60601-1:2005, *Medical electrical equipment, Part 1: General requirements for basic safety and essential performance*, 2005 OR *Clause 14* of ANSI/AAMI ES60601-1:2005, *Medical electrical equipment, Part 1: General requirements for basic safety and essential performance*, 2005 (adoption with national deviations of IEC 60601-1:2005).
- IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2010.

Thank You!