Panel 3
Al-Aswad
Reites
Karandikar
Myung
Sharon

PANEL 3: Effective safeguards and methods for mitigating the risks for an ophthalmic digital health device and the assets, threats, and vulnerabilities to be considered and identified

Moderators
Mark S. Humayun, MD, PhD
Derek T. Sprunger, MD
3. What are the most effective methods of mitigating risks for an ophthalmic digital health device?

   a. Safeguards built into the software;
   b. Safeguards built into the hardware such as:
      i. Light standards for light sources
      ii. Electrical and EMC standards
   c. Methods to limit the intended users
   d. Labelling for patient use
   e. Training modules and tutorials

4. What are the assets, threats, and vulnerabilities that should be considered and identified as a threat to the privacy of a patient by ophthalmic digital health device developers?

   a. Transmission of information to electronic medical records or other databases
   b. Storage of information on the personal device or cloud devices
   c. Monitoring patient behavior and location
Tele-ophthalmology

Lama A. Al-Aswad, MD, MPH
Associate Professor of Ophthalmology
Director, Tele-ophthalmology Initiative
Director, Glaucoma Fellowship
Chair of Quality Assurance
Columbia University College of Physicians and surgeons
What are the most effective methods of mitigating risks for an ophthalmic digital health device?

Methods to limit the intended users

- All users are issued individual user ID’s and Passwords to the application, network and server by the system administrator
- Users are required to change passwords every 90 days
Labelling for patient use

- Participants do not require a user ID or password the privileges are very restrictive only allowing entering information on specific screens and prohibits users from viewing other patient data or altering data.

Training modules and tutorials

- We’ve developed a comprehensive training plan to accompany all users which includes:
  - pdf instructional guides to reference
  - video recordings/tutorials
  - onsite training & conducting test visits with providers
  - Screen shots
  - Retraining
  - Report card
What are the assets, threats, and vulnerabilities that should be considered and identified as a threat to the privacy of a patient by ophthalmic digital health device developers?

Transmission of information to electronic medical records or other databases

- To the server and the system has its own independent server

- The data capture software is offline to users when not in use but the server is always available
Monitoring patient behavior and location

- Mobile unit
- Virtual visits
  - NYP OnDemand requires the patient to select the state in which they currently are located prior to their Urgent Care visit
  - We explain patient is legally agreeing to be located in the state they select - which are the states our providers are licensed in
  - NYP is developing geolocation into its app that will not allow patients to enter virtual visits should they have location services enabled and are located outside of an allowed state.
JOHN REITES
Partner & Chief Product Officer
THREAD (www.THREADresearch.com)

Executive intrapreneur turned digital health entrepreneur. John’s career includes over 15 years leading global drug development and healthcare innovation. Named one of the Top 100 Influencers in Digital Health, John provides expertise and execution experience in digital health strategy, remote patient research and care, virtual clinical trials, Phase I - IV clinical research, patient reported outcomes, patient engagement, mobile health, omni-channel experience and virtual reality.

John is a keynote speaker at global industry events, guest lecturer at Duke University on digital health/innovation and a published author featured in various conferences, journals, articles and media outlets.

As Chief Product Officer, Partner at THREAD, John leads THREAD’s digital health platform enabling remote patient research conducted by biopharmaceutical companies, CROs and academic researchers.
What are the most effective methods of mitigating risks for an ophthalmic digital health device?

**eDRO™**

*Electronic device reported outcome*

eDROs use the sensors within the mobile phone itself (accelerometer, gyroscope, microphone, camera etc.) to generate exploratory data around things like patient fitness, dexterity, cognitive skills and memory.

They combine a patient activity with training and active/passive data collection.

**Training modules and tutorials**

**eDRO™**

*Electronic device reported outcome*

Example for training and activity completion
What are the assets, threats, and vulnerabilities that should be considered and identified as a threat to the privacy of a patient by ophthalmic digital health device developers?

• Data transfers/APIs
• Local storage vs cloud storage
• Geolocation and similar opt-in features
• Patient authentication
• Proper oversight of behavior and potential safety events
• Personal Background
  o 25 years in software development and management
  o 15 years in health technology, developing Web and Mobile apps at Epocrates, Intuit Health, deVero and DigiSight
  o Focus: Digital health, Mobile and Data
  o Experience with:
    ➢ Enterprise systems integrations: EHR, PACS, Patient Portals
    ➢ System Security and HIPAA-Compliance
    ➢ Data Analytics and Visualization

Paxos from DigiSight Technologies

Analytics for the enterprise customer

Capture
Collaborate
Document

Cloud-based point-of-care mobile solution that enables healthcare teams to capture data, collaborate, and coordinate patient care
Modern Software Systems have multiple tiers and different points of vulnerability. Security planning must take a holistic view of the entire system.

Security and Privacy of Patient Data: Software Safeguards

- Data encryption: Mobile, server, database, transmission
- Employee training:
  - Comprehensive policies & procedures
  - Dry runs for disaster response and recovery
- Login and Access control
- Software architecture: Distributed scalability and resilience
- API security, Data backup and recovery
- External validation: Pen-testing
Threats to Patient Data Security and Privacy

Data Storage on Mobile and Cloud
- Unauthorized data access
- Abilities of Cloud Service Provider
- Potential for data loss on mobile

Data Transmission to EMR, PACS and other databases
- Patient ID matching
- Transmission and End-point security
- Multi-integration workflow
- Incomplete data sync

Mitigating Risks for Ophthalmic Digital Health Devices: Safeguards built into hardware

- Light standards for light sources
- Electrical and EMC standards

David Myung, MD, PhD
Assistant Professor
Director, Ophthalmologic Telemedicine
Co-Director, Ophthalmic Innovation Program
Byers Eye Institute at Stanford
VA Palo Alto Health Care System
Building safeguards into an ophthalmic camera system

**Disclosure:** Co-Inventor on Paxos ophthalmic camera system and Consultant to DigiSight Technologies

- Case study of a smartphone-based ophthalmic camera system
- Process of getting it registered as a 510(k) Class II Exempt device

New Product Code in 2015

In April of 2015, the FDA re-classified ophthalmic cameras into Group 1 and Group 2 determinations.
Ophthalmic Camera: Compliance Package

Optical Radiation Safety:
ISO 15004-2:2007*

Quality System:
ISO 13485:2003

Risk Management:
ISO 14971:2012

Electrical Safety:

Depending on Group 1 vs. Group 2 designation, more testing is needed. Group 1 enables classification as an “Exempt” device under 510(k) Class II, Product Code PJZ.

* ANSI Z80.36-2016 starting in 2016

---

Information to Support a Claim of Electromagnetic Compatibility (EMC) of Electrically-Powered Medical Devices

Guidance for Industry and Food and Drug Administration Staff

The draft of this document was issued on November 2, 2015.

For questions about the document, contact the Division of Biomedical Physics, Office of Science and Engineering Laboratories at 301-734-2360 or Donald Ritter at 301-734-2405 or email Donald.Ritter@fda.hhs.gov.

- Specific performance criteria based on the device functions, indications, intended use, and essential performance.
- Characterization of device immunity, and to ensure that function of the device does not interfere with neighboring devices.
- Addressing any device effects, disruptions, or degradations observed during testing and how these are mitigated.

As mobile technologies have continued to evolve, the FDA has put into place a set of straightforward guidelines for building hardware safeguards into new devices.

The two main hardware-related safety issues inherent to ophthalmic devices in this area are optical radiation safety and electrical safety/electromagnetic compatibility (EMC).

Quality System and Risk Assessments are also critical.

**Conclusions**

**OPHTHALMIC DIGITAL HEALTH WORKSHOP**

Artificial Intelligence in Effective Safeguards

Eitan Sharon, PhD
CEO & Founder, Mode.AI

AI visual bot for conversational shopping
Machine Learning Safeguards in Software

- **ML unit and holistic testing**
  - Building confidence through evaluating chances
- **ML monitoring of abnormalities in activity**
  - Detecting exception from learned patterns
- **ML supervision on the human factor**
  - Detecting imposter screens and wireless networks

ML Monitoring of Patient’s Behavior

- **Monitoring location**
  - Matching against familiar locations
- **Monitoring movement patterns**
  - Comparing with the expected
- **Monitoring behavior**
  - Understanding signals for various functioning - such as the when and whereabouts of eating, of self-care time, indoors, outdoors, traveling, etc.
Safeguards in the Storage of Information

- **Storing on the Cloud**
  - Authentication that requires a hardware component (e.g. fingerprint or face recognition)

- **Storing on Mobile**
  - Captcha; Bio Identification.

- **End to end encryption**
  - Keeping data safe in between end points