Consumer Mobile Health Application Functional Framework (cMHAFF) Overview and Update

Mobile Health
January 2017
San Antonio WGM
cMHAFF Scope and Goals

- Provide a standard as a framework for assessment of a mobile app’s foundational aspects:
  - Security
  - Privacy/consent
  - Risk assessment
  - Usability assessment
  - Data access privileges for consumers and others
  - Data export (sharing)
  - Transparency of conditions (disclosures)

- Assessment might include attestation, testing, endorsement, and voluntary or regulatory certification

- Out of scope: clinical/health content or functionality
Why cMHAFF? What’s the Need?

- **Target Audience:** mobile health app developers needing guidance on building apps
- **Beneficiaries:** consumers, providers
- **Consumers** need protection, transparency and assurance regarding mobile apps. Some examples:
  - What **security** protections exist behind that “cloud?”
  - Can I **comprehend**, or even find, privacy policy and terms of use?
  - Who can the app **disclose** data to?
  - What does the app **know** about me (location, microphone, contacts, photos, etc.), and what can it **do** on my device?
  - Can I **access** my app data like I can under HIPAA?
  - What happens to my **data** if I delete an app?
cMHAFF Exemplar Use Cases
cMHAFF Topics

- Product Development and Support
  - Risk assessment, usability, customer support

- Download and Install App
  - App store experience, establish account, launch app

- Conditions and Agreements (new)
  - Disclosures, terms, charges, in-app payments, incentives

- Use App
  - Authentication, authorization for app services, authorization for data, pairing user accounts, security for data at rest and in transit, data authenticity and provenance, product upgrades, audit

- App Service Termination
  - App & data removal, post closure use of data
Ballot: Current Status

- ~100 comments (35 negatives) dispositioned and being incorporated into new cMHAFF
- Moving toward ballot in May 2017 cycle
- Keeping Informed by inviting guests from industry efforts (e.g., ONC/Accenture Patient-Generated Health Data; ONC Model Privacy Notice; SMART on FHIR; FTC Consumer Protection and Disclosure…)
Current Project Plan

- Usability, Notifications, Wordsmithing (done)

- January-February 15: Security and Privacy (encryption, auditing, authorization, consent, etc.) to be refined by collaborating with Security and CBCC workgroups

- Feb 15-March 6: Regulatory and best practice references

- March 6-31: New material from industry developments, formatting, editing, NIB for May ballot
cMHAFF Motivation - Invitation

- This is an exciting new opportunity in an exploding space: get in on the ground floor!
- We have leeway to make broad changes to meet emerging needs
- Help us take a right-sized approach, addressing important gaps without stifling innovation or being too prescriptive
- Help HL7 collaborate well with the public and private sectors
Project and Contact Info

- Meets on Mondays at 5pm Eastern
  - Webex
    - [https://westat.webex.com/westat/j.php?MTID=mbd682bcdce33caf6ad89daaad8841d6f](https://westat.webex.com/westat/j.php?MTID=mbd682bcdce33caf6ad89daaad8841d6f)
  - Phone 770-657-9270, passcode 465623

- Project Leads: Nathan Botts / David Tao

- **Join us** to move cMHAFF forward!
Backup Slides
Mobile App Lifecycle

cMHAFF is based on app lifecycle from download through deletion from device
cMHAFF and API Task Force Scope

- **API Task Force**
  - Provider/EHR perspective
  - Constrained MU3 focus
  - Recommendations re regulatory oversight
  - App registration (deployment)
  - App endorsements and experience sharing via secondary market
  - Model Privacy Notice
  - Model Authorization Form
  - Ability of provider, patient, and app to restrict access
  - Auditing and accounting of disclosures in EHR
  - Identity-proofing

- **Both**
  - Consumer device connected to EHR via API
    - Read-access to EHR
    - Assess applicable regulations
    - Communication of app’s privacy policies and practices
    - Usability and Accessibility
    - Patient/User authorization (consent)
    - Auditing of access
    - User authentication
    - App authorization
    - Security for data at rest (for EHR, already covered in certification)
    - Security for data in transit

- **cMHAFF**
  - Consumer/device perspective
  - Use Case: Simple Standalone App
  - Use Case: Device-connected wellness app
  - Broad focus
    - Write-access to EHR
    - Product risk assessment and mitigation
    - Product usability
    - Customer Support
    - Download and install App
    - Launch App and establish user account
    - Authorization for use of smartphone services
    - Pairing user accounts w. devices/repositories
    - Data authenticity and provenance
    - In-app payments
    - Notifications and alerts
    - Product upgrades
    - Reward and incentives
    - App testing and certification to standards
    - Auditing on consumer device **(note: “accounting of disclosures” not covered)**
    - App and data removal
    - Permitted uses of data post closure