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

Mobile Health
September 2016
Working Group Meeting
Why cMHAFF? What’s the Need?

- Consumers need protection, transparency and assurance regarding mobile apps. Some examples:
  - Who else 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 clinical **evidence** underlies this wellness app?
  - What **security** protections exist behind that “cloud?”
  - Can I **comprehend**, or even find, privacy policy and terms of use?
  - What happens to my **data** if I delete an app?

- Developers need guidance on building MH apps

- Benefits: consumer and provider confidence in the apps, and assistance to developers
cMHAFF Scope and Goals

- Provide a standard against which the security and privacy of a smartphone (or tablet) app can be assessed
- Promote the generation of health data which is reliable, actionable, and accessible by consumers
- Promote transparency for consumers to understand what their apps do with their data
- Framework does not address the specific health content/functionality of an app
cMHAFF Exemplar Use Cases

<table>
<thead>
<tr>
<th>Simple</th>
<th>Device Integrated</th>
<th>EHR Integrated</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDA App Categorization</td>
<td>wellness</td>
<td>wellness</td>
</tr>
<tr>
<td>Device Data Collection</td>
<td>none</td>
<td>unregulated device</td>
</tr>
<tr>
<td>PHI Data Storage</td>
<td>smartphone</td>
<td>smartphone/PHR</td>
</tr>
<tr>
<td>Data transmission by App</td>
<td>none</td>
<td>device-app-PHR</td>
</tr>
<tr>
<td>Importance of Data Integrity</td>
<td>low</td>
<td>mid</td>
</tr>
<tr>
<td>HIPAA covered?</td>
<td>no</td>
<td>no, but yes, if white-labeled</td>
</tr>
</tbody>
</table>
Mobile App Lifecycle

cMHAFF is based on app lifecycle from download through deletion from device

START

Navigate to an app store and search for app to download

Review privacy policy and app content

Download app

Launch app and establish user account

Use app, which generates user data and metadata

Extend usefulness of app (add proxies, associate accounts, provision devices, direct data)

Discontinue use of app

Delete app

END
cMHAFF Topics

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

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

- **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, in-app payments

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

- 104 ballots received (many referring to the same spreadsheets), 30 negatives, 32 affirmative, 42 abstentions
- ~100 comments (35 negatives) received and dispositioned
- Ballot reconciliation approved by project team
- Next step: rewrite cMHAFF to move toward STU ballot (target 1H 2017)
Ballot Comment Themes (1)

- Scope of regulation vs certification vs testing vs guidance
- US Realm vs International Realm
- Need for more specific, testable, criteria, including reference to other standards
- “Guidance” vs “standards” (conformance statements)
- Debate about appropriateness of guidance in non-technical areas, e.g., terms of agreement
- Loosening or tightening some conformance statements
- Challenges establishing universal (vs conditional) conformance, considering huge diversity of “health” apps purposes, intended users, and connections to EHRs
Ballot Comment Themes (2)

- Balancing usability vs stringency (e.g., notifications, alerts)
- Assessing developer burden, considering the landscape of small app developers
- Referencing other guidance, e.g., OCR, FTC, HIPAA, FDA, COPPA, NIST
- Applicability (or not) of other HL7 standards, e.g., FHIR, EHRS-FM, CDA, v2, in MH space
- Need for more examples
Addressing US-realm Gaps

- Opportune time for HL7/cMHAFF to consider
  - FTC/OCR Guidance
  - HIT Joint Committees API Task Force
  - ONC Report: Gaps in Oversight of Non-Covered Entities (MH apps, social media, PHRs)
  - ONC PHR Model Privacy Notice: applicable to MH?
  - MH platform-specific guidelines (e.g., new for iOS)
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
cMHAFF Motivation - Invitation

- This is an exciting new opportunity in an exploding space: get in on the ground floor!
- Comment-only cMHAFF ballot permits 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
  - Phone 770-657-9270, passcode 465623

- Project Leads: Nathan Botts / David Tao

- Join us to move cMHAFF forward to STU!