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

Mobile Health

May 2017

HL7 Madrid WGM

cMHAFF Scope and Goals

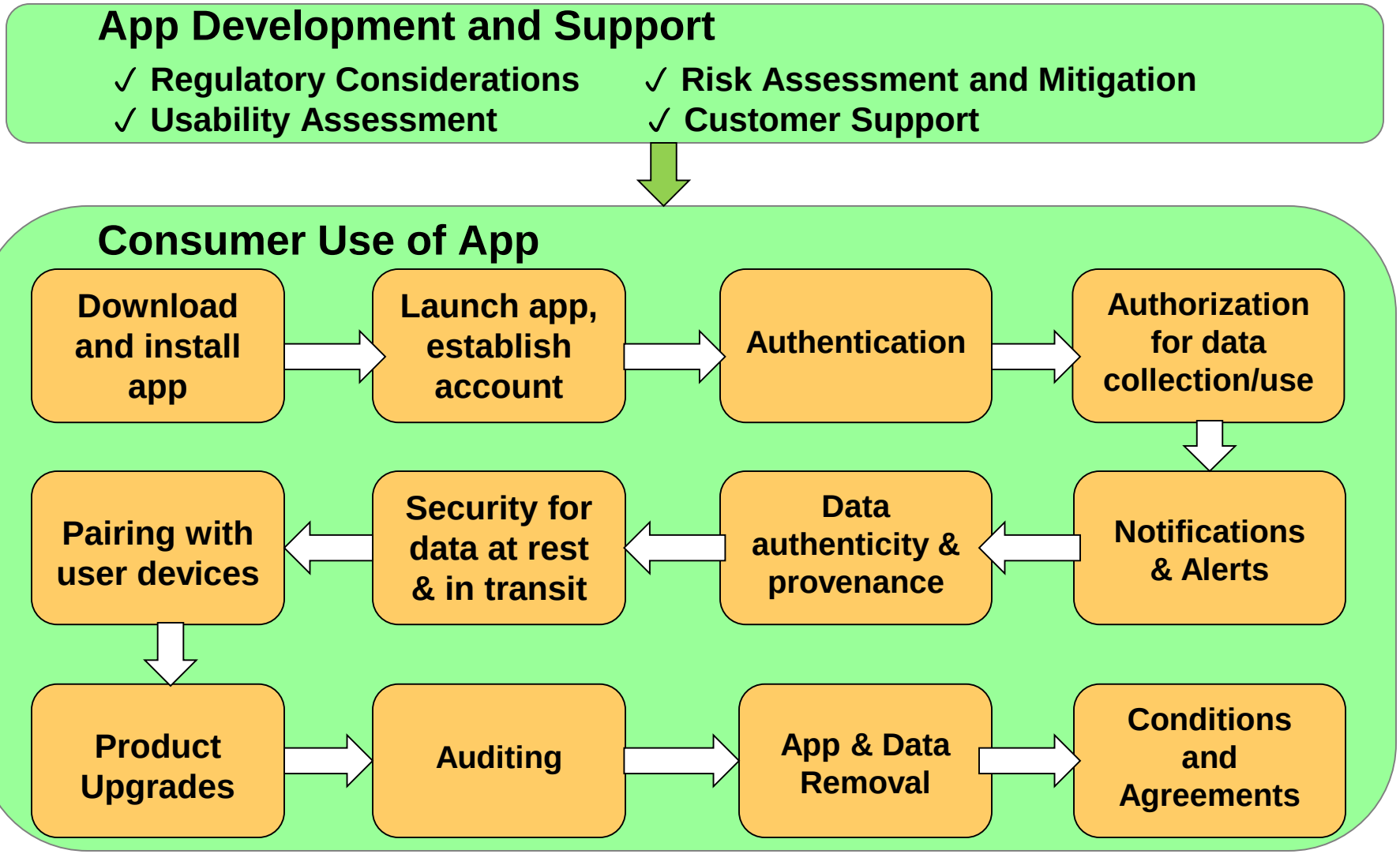
- Provide a framework for assessment of the **common foundation** of mobile apps
  - Security
  - Privacy/consent
  - Risk assessment
  - Usability assessment
  - Data access privileges
  - Data export (sharing)
  - Transparency of conditions (disclosures)

- Assessment might include attestation, testing, endorsement, and voluntary or regulatory certification
- Out of scope: clinical/health content or functionality

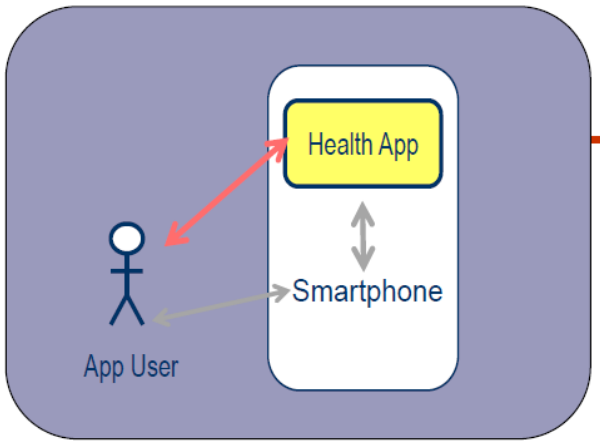
Why cMHAFF? What's the Need?

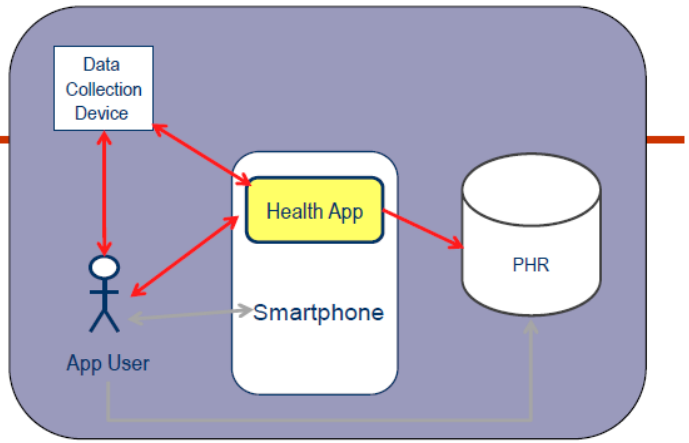
- Target Audience: **mobile health app developers** needing guidance on building apps
- Beneficiaries: consumers, providers
- Consumers need protection, transparency and assurance regarding mobile apps. Some examples:
  - What **security** protections exist behind that "cloud?"
  - Can I **comprehend**, 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?

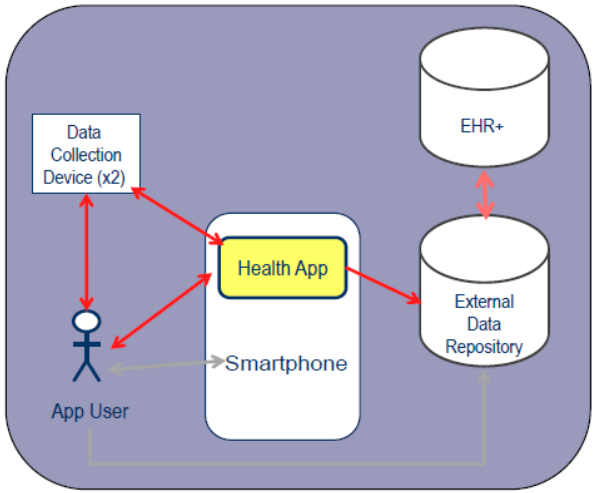
cMHAFF Sections and App Life Cycle



cMHAFF Exemplar Use Cases







	Simple	Device Integrated	EHR Integrated
FDA App Categorization	wellness	wellness	medical
Device Data Collection	none	unregulated device	FDA regulated device
PHI Data Storage	smartphone	smartphone/PHR	cloud/EHR
Data transmission by App	none	device-app-PHR	device-app-cloud-EHR
Importance of Data Integrity	low	mid	high
HIPAA covered?	no	no, but yes, if white-labeled	yes

EHR-Integrated Use Case "C"

A diabetes management app allows a consumer to collect blood sugar readings through a Bluetooth-enabled glucometer. The app is offered by the provider, a HIPAA covered entity. Its purpose is to allow the patient's blood sugar to be captured through devices, rather than relying on manual entry by the patient, and to electronically transmit the readings to the patient's physician, rather than relying on paper or FAX logs. Activity information is collected through an activity tracker, and a consumer can open the app and tap icons when they have a meal or a snack to enable estimates of caloric consumption. Collected data is automatically "pushed" to a third-party cloud-based platform. The patient is aware of the cloud platform, though not familiar in detail with how data are protected in transit or as stored. When a consumer views information on their smartphone which shows daily glucometer readings and related information, this information is "pulled" into the app but does not persist on the smartphone when the app is closed. It is also possible for the consumer to directly enter blood sugar readings (e.g., using backup manual glucometer if Bluetooth device is not working). From the cloud platform, consumer information is "pushed" to a provider's Electronic Health Record (EHR) of the patient, where it is accepted as Patient Generated Health Data (PGHD), according to the preferences of the patient and the policies of the provider. From the EHR, a physician can set upper and lower boundaries for blood sugar readings such that the consumer is alerted through the app when a measurement is out of range. From the EHR a physician can create logic which sends an alert to the consumer's care manager when a set number of high or low readings are noted within a prescribed period of time. The "consumer" and the "patient" are the same person in this example. From the EHR's perspective, the record is a patient record.

Changes Since January

- ~100 comments (35 negatives) dispositioned and being incorporated into new cMHAFF
- Expand Security Risk Analysis, informed by:
  - Collaboration with HL7 Security and CBCC Workgroups: HL7 Security Risk Assessment Cookbook
  - Other Related Industry Initiatives
- Moving toward September 2017 Ballot

Related Industry Efforts

ONC ISA Task Force and PGHD Whitepaper

NIST National Institute of Standards and Technology U.S. Department of Commerce

HITRUST 10 YEARS 2007-2017 INNOVATION. PROTECTION.

OWASP Mobile Top 10 Security Risks

SMART® on FHIR®©

FTC/FDA/OCR Mobile App Developer Guidance Tool

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
  - GoToMeeting https:/www.gotomeet.me/dtao
  - Phone 770-657-9270, passcode 465623
- Project Leads: David Tao / Nathan Botts
- **Join us** to move cMHAFF forward!