MOBILE HEALTH APPS CONFORMITY ASSESSMENT & CERTIFICATION GUIDANCE CONCEPT NOTE

Author: Gora Datta, FHL7, SMIEEE, SMACM <gora@cal2cal.com>

BACKGROUND
The proliferation of Digital Health tools, including mobile health apps and wearable sensors, holds great promise for improving human health⁷. The impact of Digital Health on patient care is accelerating with the increasing adoption of mobile health apps and wearable sensors. As per US-FDA: “The broad scope of digital health includes categories such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine.”

As of 2019, there are between 400,000 to 500,000² health, wellness and fitness apps that run on smartphones, watches, tablets, and other mobile devices, available for download from platform-specific application stores such as the Apple App Store (iOS) and Google Play (Android). This number has rapidly grown from 325,000³ apps in 2017.

It is envisaged that soon we will have clinicians prescribing mobile health apps to patients, similar prescribing medicines or medical devices⁴. In fact, Germany will soon pass a law in 2020⁵ that will enable German doctors to prescribe health apps⁵. Other countries are also marching down this path.

However, before this becomes as common as prescribing a medicine or a medical device by a provider, the mobile health app needs to safe/secure/accurate not only for the individual user/patient/family member but also for the clinician/payer/provider/regulatory community. Given the era of cybersecurity and its impact on healthcare⁶, it is critical that the healthcare informatics standards community looks into this matter now.

PROBLEM
Mobile health apps have access to highly detailed, personally identifiable and clinical information about end-users. Security and privacy are big issues, raising questions about permission control and confidentiality, as well as the integrity of the infrastructure and the individual. There is also a need to clarify how to ensure practicalities of data storage and management, availability and maintenance of the network, as well as compatibility and interoperability.⁷

However, there is no established mobile health app certification process. It is a possibility that we will see a proliferation of non-standardized, country-specific, siloed certification process being established over the next few years. We are already seeing efforts⁸ in this area.

---

1 https://www.fda.gov/medical-devices/digital-health
6 https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/
7 https://www.himss.eu/himss-taxonomy-topics/mhealth/?page=1
STANDARDS IN THIS AREA

In June 2018, HL7® released a STU (Standards for Trial Use) that provides guidance to mobile health app developers in developing a safe and secure mobile health app:

**HL7 Consumer Mobile Health Application Functional Framework (cMHAFF), Release 1**

- The primary goals of cMHAFF are to provide a standard against which a mobile app’s foundational characteristics -- including but not limited to security, privacy, data access, data export, and transparency/disclosure of conditions -- can be assessed.
- The framework is based on the lifecycle of an app, as experienced by an individual consumer, from first deciding to download an app, to determining what happens with consumer data after the app has been deleted from a smartphone.
- The HL7 confluence project site is: [https://confluence.hl7.org/display/MH/cMHAFF+Project](https://confluence.hl7.org/display/MH/cMHAFF+Project)
- Additional/current information about cMHAFF is available here: [https://cmhaff.healtheservice.com/](https://cmhaff.healtheservice.com/)

cMHAFF is primarily directed at developers and vendors of mobile health apps for consumers, to assist them in building and marketing apps that educate consumers and protect their privacy, security, data access, etc.

The standard will not address the clinical content of such apps (e.g., "Does it give good advice?"), but will provide a framework for security, privacy, and the integration of data generated from apps into Personal Health Record (PHR) and Electronic Health Record (EHR) systems, as well as into other types of data repositories (e.g., personal data stores, population care systems). Health Apps reference applications running typically on smartphones, but also on other consumer devices such as watches, fitness devices and tablets.

cMHAFF provides a framework for assessment of the **common foundations** of mobile health apps:

- Product Information (disclosures/transparency)
- Security (including individual integrity)
- Privacy/consent/authorization
- Risk assessment/analysis
- Data access privileges
- Data exchange/sharing
- Usability & Accessibility

Assessment could include attestation, endorsement, testing, voluntary or regulatory-driven certification.
CMHAFF focuses specifically on consumer mobile apps that run on devices such as smartphones, tablets, and wearables. It is focused on the general capabilities, that can be thought of as “horizontal” features that are applicable to most or all apps, rather than to the specific health, clinical, or medical functionality of an app.
The key domains covered by cMHAFF are:

### CMHAFF Domains

<table>
<thead>
<tr>
<th><strong>Functional Requirements</strong></th>
<th><strong>Non-Functional Requirements</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Usability &amp; Accessibility</td>
<td>- Data Exchange and Interoperability</td>
</tr>
<tr>
<td>- Download &amp; Installation Considerations</td>
<td>- Product Upgrades</td>
</tr>
<tr>
<td>- App Launch &amp; Registration</td>
<td>- Audit</td>
</tr>
<tr>
<td>- App Use &amp; Operation</td>
<td>- App and Data Removal</td>
</tr>
<tr>
<td>- Consent for Data Collection</td>
<td>- Permitted Uses of Data Post Account Closure</td>
</tr>
<tr>
<td>- Account Synchronization</td>
<td></td>
</tr>
<tr>
<td>- Security for Data at Rest</td>
<td>- Non-Functional Requirements</td>
</tr>
<tr>
<td>- Security for Data in Transit</td>
<td>- Product Risk Assessment &amp; Mitigation</td>
</tr>
<tr>
<td>- Data Authenticity, Provenance, and Associated Metadata</td>
<td>- Regulatory Considerations</td>
</tr>
</tbody>
</table>

There is also an ongoing ISO/TC215 TS:ISO 82304-2 Quality Criteria for Health and Wellness Apps[^9] that is currently under way. The project team intends to present their work as a Technical Specification (TS) by November 2020. **The project was commissioned by EU Commission as “Health and Wellness Apps – Quality and reliability criteria across the life cycle – Code of Practice”**.

THE DRAFT TECHNICAL SPECIFICATION IS SLATED TO BE RELEASED IN OCT/NOV 2022.

---

cMHAFF mLabel: Labelling of Apps

A key feature of cMHAFF is mLabel – a visual summary of the features of the app. This will aid in its assessment whether by an end-user or by a prescriber/regulator. This is very similar to the well-known food product “Nutrition Facts” or “Drug Facts” labels, as depicted below, we all are well accustomed to.

For cMHAFF, each “topic” (the sections of conformance criteria) would be represented by an entry, for example a table. We envision an easy-to-understand combination of graphical symbols and colors (red = bad/fail, yellow = middle/partial, green = good/present, gray = not applicable). The label’s information would be provided by a combination of self-attestation (by the app provider) verified by a third party (e.g., assessment or certification body), and possibly supplemented by third party testing (e.g., technical requirements for interoperability, security, etc.).

Here is a future/projected view of cMHAFF: mLabel
Unlike Nutrition Fact or Drug Fact labels, mLabel is dynamic in nature. Its digital representation will allow for representing local/regional/country-specific information and regulations. The hyper-link capability, when present on a mobile device (as a part of a mobile health app), will allow the user to quickly drill-down and locate additional information about the app.

ISO/TC215 WG1, in collaboration with HL7 Mobile Health WG, is evaluating developing an ISO/TC215 technical specification (TS) document for mLabel.

CONFORMITY ASSESSMENT\textsuperscript{10,11}

IEEE Conformity Assessment Program (ICAP) develops and implements programs that couple standards development activities with conformity assessment activities to help accelerate market adoption while reducing implementation costs.

Conformity assessment involves a set of processes that show your product, service or system meets the requirements of a standard. When applied to product, it involves testing to an established performance standard, as well as inspection, quality management, surveillance, accreditation and declaration of conformity. Undergoing the conformity assessment process has a number of benefits:

- It provides \textit{consumers} and other stakeholders with added confidence, security and integrity.
- It gives your \textit{company} a competitive edge.
- It helps \textit{regulators} ensure that health, safety or environmental conditions are met.

RECOMMENDATION

It is recommended that a “consortium” of following entities be established to create standards to address issues related to a uniform conformity assessment framework and subsequent certification of mobile health apps:

- IEEE Standards Association (lead entity)
- ISO/TC215
- ISO CASCO
- CEN/TC251
- HL7 International
- ITU-T
- US-FDA (Food & Drug Administration)
- EU-EMA (European Medicines Agency)
- HIMSS
- IHE
- WHO
- US-NIST
- International Medical Device Regulators Forum (IMDRF)
- Multilateral Agencies
  - The World Bank

\textsuperscript{10} https://standards.ieee.org/products-services/icap/index.html#programs
\textsuperscript{11} https://www.iso.org/conformity-assessment.html
Asian Development Bank
• African Development Bank
• Other competent international authorities/bodies

As notes earlier in the document, not having a collaborative approach amongst various global stakeholders runs the risk of seeing a “proliferation of non-standardized, country-specific, siloed certification process being established over the next few years” in the mobile health app space.

Another aspect that was briefly mentioned earlier and is critical for mobile health app usage, by both patients and healthcare providers, is the impact of cyber security on these apps.  

Author:
Gora Datta, FHL7, SMIEEE, SMACM
goradatta@ieee.org

• (founding) Co-Chair HL7 Mobile Health
• Convenor ISO/TC215 Standards & Conformance
• Convenor ISO/TC215 WG#10 Traditional Medicines
• Convenor ISO/TC215 Outreach & Communications
• Chair IEEE Healthcare: Blockchain & AI Virtual Series
• Chair SUSTECH2021: 8th IEEE Conference on Technologies for Sustainability
• Chair IEEE Southern California Council
• Chair IEEE Southern California CyberSecurity
• Secretary IEEE-USA US Government Communities of Interest (USG CoI)
• Treasurer IEEE Orange County Section
• Vice Chair IEEE OC Section EMBS Chapter
• Industry Director, Smart Pandemic Management, University of California @ Berkeley
• Executive Director, P3 Innovation Center (CA based non-profit)