Nathan Botts, PhD, MSIS
Co-Chair, Mobile Health Work Group, Westat

Frank Ploeg
Co-Chair, Mobile Health Work Group,
University Medical Centre Groningen

Gora Datta
Co-Chair, Mobile Health Work Group, Cal2Cal

Matthew Graham
Co-Chair, Mobile Health Work Group, Mayo Clinic

Function List Component Descriptions

The Function List includes the following components:

Function ID # (Normative)	This is the unique identifier of a function in the Function List (e.g. CP.1.1) and should be used to uniquely identify the function when referencing functions. The Function ID also serves to identify the section within which the function exists (CP = Care Provision Section) and the hierarchy or relationship between functions (CP.1.1 is a sibling to CP.1.2, parent of CP.1.1.1 and child of CP.1). In many cases the parent is fully expressed by the children.
Function Type (Reference)	Indication of the line item as being a header (H) or function (F) or conformance criteria.
Header/Function Name (Normative)	This is the name of the Function and whilst expected to be unique within the Function List; it is not recommended to be used to identify the function without being accompanied by the Function ID. Example: Manage Medication List
Function Statement (Normative)	This is a brief statement of the purpose of this function. Whist not restricted to the use of structured language that is used in the Conformance Criteria (see below); the Statement should clearly identify the purpose and scope of the function. Example: Create and maintain patient-specific medication lists.
Description (Reference)	This is a more detailed description of the function, including examples if needed. Example: Medication lists are managed over time, whether over the course of a visit or stay, or the lifetime of a patient. All pertinent dates, including medication start, modification, and end dates are stored. The entire medication history for any medication, including alternative supplements and herbal medications, is viewable. Medication lists are not limited to medication orders recorded by providers, but may include, for example, pharmacy dispense/supply records, patient-reported medications and additional information such as age specific dosage.
Conformance Criteria (Normative)	Each function in the Function List includes one or more Conformance Criteria. A Conformance Criteria, which exists as normative language in this standard, defines the requirements for conforming to the function. The language used to express a conformance criterion is highly structured with standardized components with set meanings.
R1.1 Reference (Reference)	Reference to the previous version of the Functional Model is included to support transition from one version to the next. The first 2 digits indicate the source document; FM = Functional Model, LM = Lifecycle Model. The remainder of the reference is to the function and, if applicable, conformance criteria.
Change Indicator	The change indicator shows the change from previous versions. This will be valued as follows: C - Changed D - Deleted N - New NC - No Change
Row #	A unique number for the row within the section.

Introduction and Overview

Acknowledgements
The Consumer Mobile Health Application Functional Framework (cMHAFF) team acknowledges the members of the HL7 Mobile Health Workgroup, who developed this Standard for Trial Use. In addition, acknowledgements are due to the HL7 EHR Workgroup and the HL7 Security Workgroup, and the Community Based Health Services (CBHS) workgroups, which also provided valuable guidance. Many other mobile health initiatives in the European Union and USA influenced cMHAFF as well, as referenced throughout this specification.

Background
As of 2021, there are thousands of consumer health applications (apps), which 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). Consumer acceptance and use of these apps is primarily based on recommendations—either personal recommendations through individual contacts or social media or app store ratings. While this information is important in understanding the relevance of an app to one's life and the design and usability of an app, it is insufficient in communicating how an app secures and protects the personal information of its users. This poses a problem both for consumers and clinicians, who may be considering or prescribing use of an app to help track and improve health behaviors and conditions.

There is a great diversity in consumer health apps. Some are meant to be used for oneself, some help manage care for others, and some work best when an individual uses an app along with consultation from a health professional. Below are three exemplary use cases of increasing complexity that are introduced and serve to guide development of cMHAFF.

Intended Audience
1. 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.
2. cMHAFF is also directed at organizations (such as test labs, certification bodies, professional societies, or organizations that provide app reviews and ratings) that will assess or endorse mobile apps for conformance to essential criteria.
3. cMHAFF can also be informative as a checklist (or "gold standard") for prospective purchasers of mobile apps (e.g., consumers, or providers on behalf of consumers).

The beneficiaries of cMHAFF will primarily be consumers, due to improvements in apps and in a consumer's increased understanding and trust. Other beneficiaries may include those who receive information from consumer health apps, such as providers, caregivers, and researchers. Some provider organizations, such as the American Medical Association, have published principles1 to ensure accurate, effective, safe and secure mHealth apps.

Relationship to Other Standards
- The HL7 EHR System Functional Model and the HL7 PHR System Functional Model, and their profiles, provided inspiration for cMHAFF. While cMHAFF is not intended for EHRs and PHRs, it is similar in that it is a broad general framework that can be constrained or extended (profiled) to focus on specific realms or types of apps.
- Several European standards and guidelines for mHealth apps were analyzed and mapped to cMHAFF categories. These are included in Section 7.0, References.

How to Use this Guide
The questions in this section help the intended audience (particularly mobile app developers and vendors) determine which conformance subsections of cMHAFF should be read. Each subsection contains one or more conformance statements. Based on the characteristics of the app being developed, some of those subsections may be applicable and some may not. To assist developers in understanding which subsections of cMHAFF are relevant to their app, the following table is presented. The left column is a yes/no question, and the right column represents decisions whether or not to apply sections of cMHAFF, depending on the answer to that question.

QUESTIONS	DECISIONS BASED ON ANSWERS
As a mobile app developer, what sections apply to me no matter how simple the app?	Product Development, Product Upgrades, Download and Install App

Does the app handle patient-identifiable information?	YES – then cMHAFF sections on authentication, authorization, audit, app and data removal, and permitted uses post closure apply NO – then those sections from cMHAFF do not apply
Does the app store or transmit data outside the mobile device, e.g., the cloud or another HIT system?	YES – then cMHAFF security for data at rest, security in transit, data authenticity and provenance and data exchange and interoperability apply
Does the app connect to sensors or other types of devices that gather measurements of the patient's condition?	YES – then cMHAFF pairing and syncing also apply
Does the app send alerts or notifications to the user?	YES – then cMHAFF notifications and alerts applies

For the September 2021 HL7 ballot, reviewers were asked to:

1. **Make recommendations concerning conformance criteria, particularly the SHALL vs SHOULD vs MAY**
2. **Extend lists of resource references, including references to other normative and emerging standards**
3. **Review the framework for broad applicability and ability to be profiled in different countries.**

The intent of the Mobile Health Work Group is to use this feedback to improve the quality and relevance of the Framework so that it can be approved as a Standard for Trial Use 2 (STU) in 2023.

Each section addresses product information and technical concerns based on a given stage of the app lifecycle, through conformance criteria, supported by references to related regulations and standards. Implementation guidance is also included.

Goals

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. It is important to note that the Framework does *not* speak directly to the specific health or clinical functionality of an app but can be extended to do so through the use of profiles (with constraints and/or extensions) developed on top of cMHAFF.

The decision to create a standard focused on a smaller set of criteria was made so that the standard is both developer-friendly and easy to update on a frequent basis. CMHAFF challenges market assumptions concerning safe and acceptable use of personal information and may in some circumstances increase coding complexity and decrease the efficiency of data transmission. As such, there is no expectation that most consumer health apps will choose to follow this standard. Yet, for apps which conform, cMHAFF can potentially provide a path to assessments that can span a range including self-attestation, testing, endorsement[2], and/or certification (voluntary or regulatory). CMHAFF is independent of the method of assessment but aims to be suitable for use for types of assessments up to and including certification. Certified apps can promote their conformance, and as a consequence, consumers who use the apps, and providers who recommend them, can be more confident of an app's rigor in enforcing basic security, its respect for the privacy of individuals, and the usefulness of data for improving and maintaining a better state of health.

Scope

CMHAFF focuses specifically on consumer mobile apps that run on devices such as smartphones, tablets, and wearables. With that said, it is understood that "mobile" is relative and so in certain circumstances health apps running on laptops, desktops, etc, may also be included. 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.

There is a broad range of apps that cMHAFF intends to cover, from simple self-contained standalone apps that a consumer can use for personal benefit, which do not exchange or store data outside the mobile device; to apps that share or store data externally (e.g., in the app provider's cloud) but do not interact directly with provider systems; to systems that share and store data externally and interact with provider EHRs or organizations (in the USA, covered entities or business

associates governed by HIPAA and/or FDA).

The intent is to lay a foundation, on top of which realm-specific and domain-specific "profiles" can be layered, that addresses an app's:

- Product Information for consumers (e.g., App Store descriptions, product disclosures)
- Security
- Privacy
- Permission to use device features
- Data Access
- Data Sharing
- Terms of Use, Conditions
- Product Development, including risk management, user-centered design, compliance with applicable regulations, functions (product description), reliability, performance, scalability, safety, compatibility, and portability.

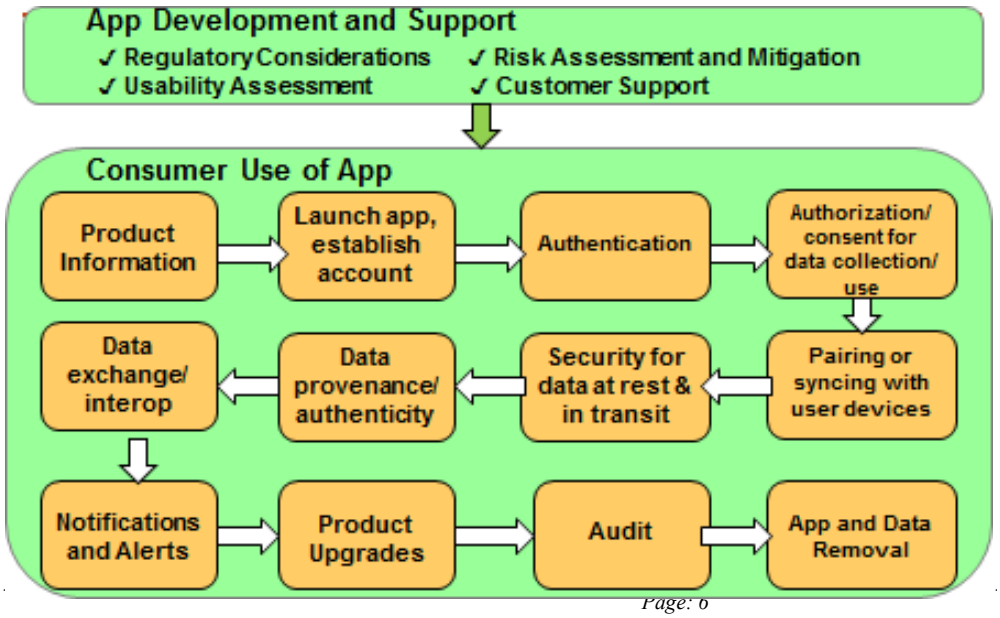
Out of Scope

- "Professional" apps that may run on consumer devices, but are intended for healthcare workers, e.g., clinical decision support aids, which are exclusively not consumer-focused.
-
- Clinical functionality of health apps (e.g., diabetes monitoring, exercise calculations). The Mobile Health workgroup does not have the subject matter expertise to define clinical-level types of criteria. These types of criteria would be outlined within specific implementation guides for use of consumer health apps in respective domains.
- General "device" security requirements, e.g., password or biometric locking of a phone. CMHAFF is an *application* functional framework intended for app developers, not a framework for the devices or platforms on which the apps run. As such, cMHAFF is not directed to Apple, Google, Samsung, or other device manufacturers and in general, seeks to remain agnostic in terms of platform. However, risk management should identify dependencies or assumptions about the common platforms that an app may rely on.
- General "infrastructure" requirements for consumers or healthcare organizations, such as the protection of networks via virus or malware protection, firewalls, etc., physical environmental security, since app developers have no control over such networks or environments. However, risk management should identify dependencies or assumptions about the supporting infrastructure that an app may rely on and should identify threats and mitigate risks.
- Human resource policies and procedures of developers, healthcare organizations, or consumers, such as security awareness education, except inasmuch as they directly affect product development.

Conformance Design Principles

Conformance Criteria in the following sections follow a lifecycle model in relation to a consumer's use of a mobilehealth application, from first finding an app in an App Store to disuse and de-installation.

Figure 1. CMHAFF Sections and Mobile App Life Cycle



Exemplary Use Cases

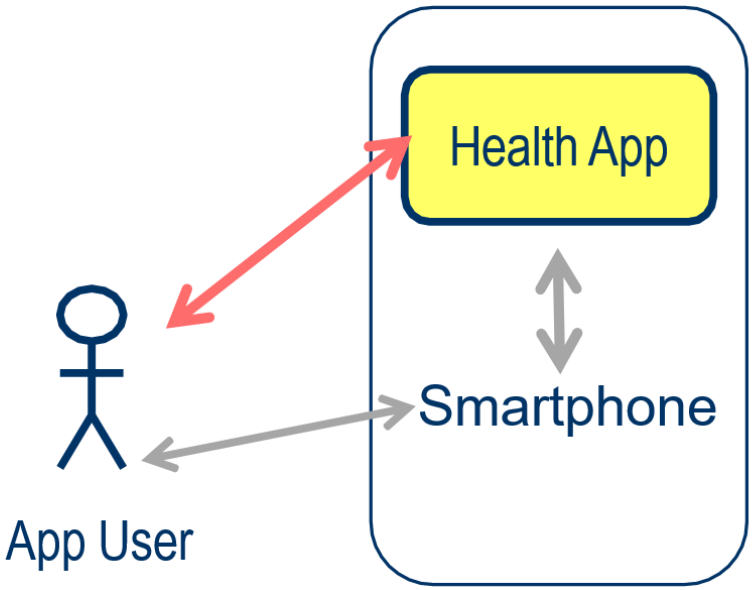
As noted in the Introduction, consumer mobile heath apps take many forms, and as such, conformancestatements in this standard must allow for variation based on multiple factors, including data sensitivity, the nature of conditions addressed by the app (e.g., wellness, chronic illness), and whether/how app data connect to other data sources.

In this section, three archetypal use cases are introduced. While most consumer mobile health apps will not precisely fit any of these models, the models are meant to demonstrate a continuum of issues whichmay be applied to any app. Use Case A covers the least sensitive example of a health app that collects user information, while Use Case B builds off of Case A with the inclusion of an external system through which personal data is synchronized with the device. Use Case C is the most sophisticated and generatesthe most requirements. Its description includes examples of the risk factors that should be considered by developers and users.

The Conformance Criteria section includes discussion of considerations as to how subsets of conformance criteria can be addressed in different manners, referencing the use cases in this section asa way to provide directional, rather than pinpoint, guidance.

Use Case A: Simple, Standalone

In this use case example a walking app collects data based on how far someone walks, using things such as accelerometers and GPS technology. In this app a consumer can view aspects such as a history of walks taken and summary statistics related to distance walked and estimated calories burned, etc. In this U.S.-based use case the App developer is not a HIPAA-covered[3] entity (CE) such as a healthcare provider, nor is the app a business associate of a CE (such as a hospital or physician). This type of app might be generally available in a mobile app store (e.g., Apple, Android) and downloaded by a consumer/patient for personal use.

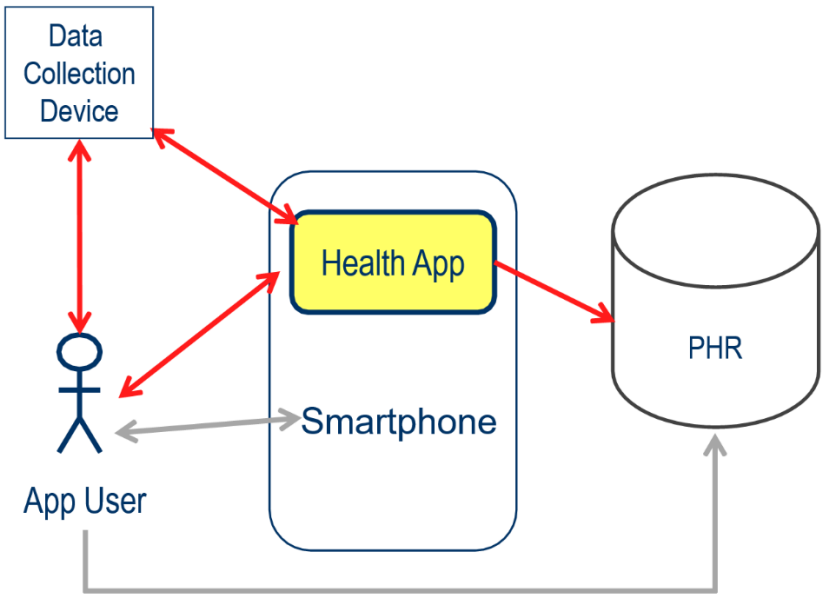


	Simple
Medical Device App Categorization	Wellness
Data Device Categorization	None
PHI Data Storage	Smartphone
Data transmission by App	None
Importance of Data Integrity	Low
(USA) HIPAA covered?	No

Use Case B: Device-Connected Wellness App

In this health app use case a weight management app is used to help consumers to systematically collect weight information, food consumption information and exercise information. Weight can be entered manually, or a consumer can

link a wireless scale to the app so that weight is automatically collected when using the scale. Food consumption is entered manually, and the tool estimates calories consumed based on the consumer's input. Exercise information may be entered manually or collected automatically through integration with a smart watch. The app analyzes all the data and offers warnings and advice (e.g., patient's unhealthy combination of weight and exercise levels lead to recommendations for diet and exercise changes). In the U.S., these types of apps, depending on their use and context could fall under FDA guidelines for Software as a Medical Device (SaMD)[1] designation, but if the health app is generally providing low-risk health lifestyle recommendations, then it would not be interpreted as a SaMD[2]. In this example, the app has an ability to download weight, activity, and food consumption information into a patient-managed personal health record (PHR) system through a published API. In the US Realm, the App developer is not a HIPAA entity, but an app developer may enter into a HIPAA business associate agreement with a covered entity and be offered to patients through an approved app store or EHR-based integration.



	Device Integrated
Medical Device App Categorization	Wellness
Data Device Categorization	Unregulated or regulated device
PHI Data Storage	Smartphone/PHR
Data transmission by App	Device-app-PHR
Importance of Data Integrity	Medium to High
(USA) HIPAA covered?	Not always. Depends on whether the PHR is owned by a covered entity.

Use Case C: EHR-Integrated Disease Management App

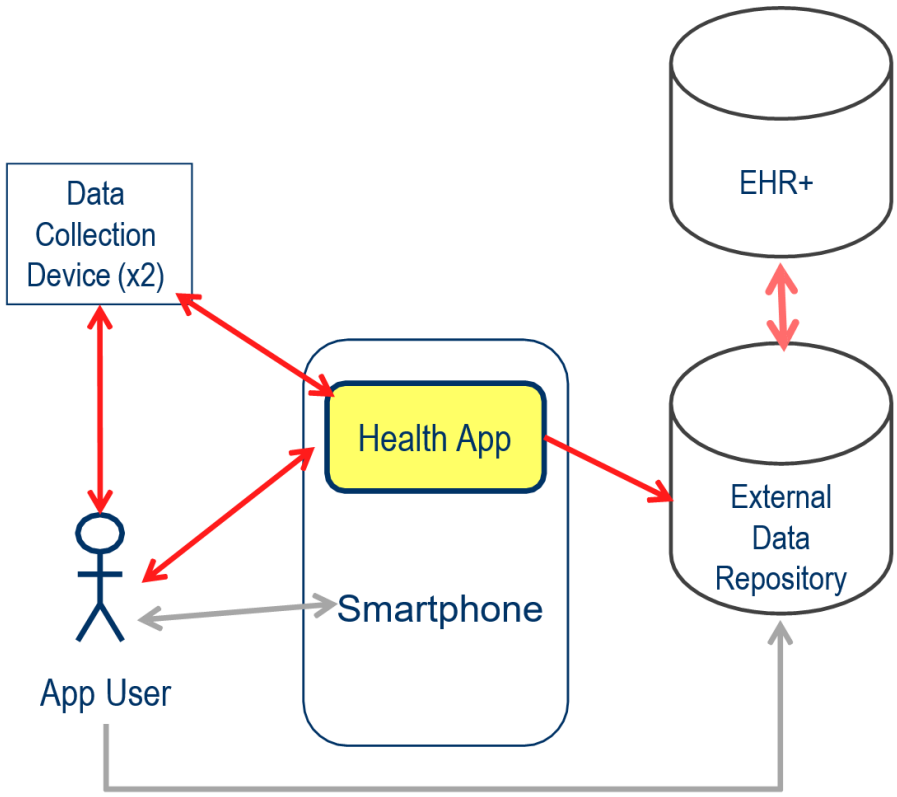
In this use case we provide the example of a diabetes management app that allows a consumer to collect blood sugar readings through a Bluetooth-enabled glucometer. A healthcare provider prescribes the app to enable the patient's blood sugar to be captured through devices, rather than relying on manual entry by the patient, and to electronically transmit the readings to the patient's physician, rather than using paper or FAX. Activity data are collected through an activity tracker, and a consumer can open the app to record meals and snacks to enable estimates of caloric consumption. This type of

[1] FDA. (n.d.). Software as a Medical Device (SaMD). Retrieved December 1, 2022, from https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd

[2] FDA. (n.d.). General wellness: Policy for low-risk devices - guidance. Retrieved December 1, 2022, from https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices

health app, integrated with a medical device would likely fall under FDA designation of SaMD and be regulated accordingly.

Collected data is automatically “pushed” to a third-party cloud-based platform. The patient is aware of the cloud, though not familiar in detail with how data are protected in transit or storage. When a consumer views information in the app, which shows daily glucometer readings and related information,this information is “pulled” in 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., if Bluetooth connection is not working). From the cloud platform, consumer information is “pushed” to a provider’s Electronic Health Record (EHR), 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 define logic to assess blood sugar readings such that the consumer is alerted through the app when a measurement is out of range or when a set number of high or low readings are noted within a prescribed period of time.



	EHR Integrated
Medical Device App Categorization	Medical
Data Device Categorization	Regulated device
PHI Data Storage	Cloud/EHR
Data transmission by App	Device-app-cloud-EHR
Importance of Data Integrity	High
(USA) HIPAA covered?	Yes

Risk Factors

For apps, especially those like Use Case C, there are several potential threats and vulnerabilities which should be assessed and mitigated, where necessary, by mHealth developers (see Product Risk Assessment and Mitigation). While cMHAFF does not attempt to "do" the risk assessment for any particular mobile app, the following are examples of specific risk scenarios that may be applicable and point to cMHAFF criteria (potential mitigations are listed in parentheses). Some of these potential risks are motivators for the conformance criteria in cMHAFF. Where risks have both high likelihood and high impact, SHALL criteria are indicated.

RISK FACTOR	CONFORMANCE SECTION
Consumer loses their device. Confidential information is handled by the app and stored on the device, leading to the risk of information disclosure (encryption of data, automatic timeout/logoff)	App and Data Removal
The device can be lost or damaged, impeding the consumer'suse of the app, thereby impacting their care, even if privacy is protected. (information about backup of data, ability to restore to new device)	Product Information
The consumer, for convenience, may turn on "automatic login" (saved credentials, "remember me"), so the app may be accessed without re-authentication. (don't offer such afeature if app handles PHI)	Authentication
The app is used and left open, where others could see it while the device is unlocked (automatic timeout/logoff)	Authentication
Measurements are not captured accurately or not transmitted accurately, and consumer takes action based oninaccurate measurements (quality management, disclosure of evidence)	Product Risk Assessment
A data collection device paired with the mobile phone may in fact be for a different person (mis-association of data) (Pairing User Accounts)	Authentication
A third-party cloud-based platform may have inadequate security measures of which the consumer is unaware. (disclosure of infrastructure security measures) Transmission between mobile app and cloud-based platform may have inadequate or unknown transmission security (encryption of data in transit)	Security for Data at Rest
The consumer exchanges or discontinues their use of the mobile device without removing all data from the device or other locations to which the device transmitted data. (App and Data Removal, Permitted Uses of Data Post Account Closure)	App and Data Removal
The healthcare provider to which the app communicates data has little or no control over the device characteristics, environment, or usage patterns, unlike enterprise IT where only approved/provisioned devices are used. (out of scope, not a developer issue, but should be documented in product risk assessment)	Product Risk Assessment

Summary of Major Differences in Use Case Scenarios

	Simple	Device Integrated	EHR Integrated
Medical Device App Categorization	Wellness	Wellness or Medical	Medical
Device Data Collection	None	Unregulated or Regulated Device	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	Medium	High
(USA) HIPAA covered?	No	No, but yes, if white-labeled	Yes

Environmental Scan

The documents mentioned below are not standards, but explain the state of the mobile health industry in the USA and Europe, and assist developers to understand which legislation is applicable to their apps.

- Journal of Medical Internet Research: mHealth and Mobile Medical Apps: A Framework to Assess Risk and Promote Safer Use https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4180335/
- HIMSS Interoperability Environmental Scan: https://www.himss.org/environmental-scan
- ONC Patient-Generated Health Data resources and references. This addresses opportunities and challenges for patient-generated health data (PGHD) and their use by clinicians. Much PGHD could come from mobile devices. https://www.healthit.gov/topic/scientific-initiatives/patient-generated-health-data.
- Good Practice Guidelines on Health Apps and Smart Devices (Mobile Health or mHealth). While this is written for France, and influenced many of the criteria in cMHAFF, it also contains an extensive literature search and references that serve as an environmental scan. https://www.has-sante.fr/portail/upload/docs/application/pdf/2017-03/dir1/good_practice_guidelines_on_health_apps_and_smart_devices_mobile_health_or_mhealth.pdf

General Considerations

Each section is a category of criteria that follows a common format. First, there is a brief non- normative description of the category. Then there is a subsection containing a normative table of **conformance criteria**. Some criteria are applicable to all consumer health apps and other criteria are to be applied conditionally based on the functionality and scope of an app. For example, some apps do not transmit personal data to a source outside of the smartphone, while some integrate with external data sources; some apps integrate with medical and wellness devices, while others do not. Criteria are separated from “force”. That is, each criterion stated in a neutral way, and the optionality of addressingthe criteria while claiming conformance to the standard, is in a separate column. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED”, “MAY", and "OPTIONAL" in this document are to be interpreted as described inInternet Engineering Task Force (IETF) RFC 2119. Force follows this convention:

- **SHALL** The definition is an absolute requirement of the specification.
- **SHOULD** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must beunderstood and carefully weighed before choosing a different course.
- **MAY** This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it orbecause the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not includethe option (except, of course, for the feature the option provides.)
- **[IF]** The stated force applies only when the clause in brackets is applicable to the product.When the clause does not apply, no conformance is expected.

Following the table of conformance criteria, there are two non-normative subsections that provideoptional guidance:

- ***Related regulations and standards***: References to documents which can help an app developeror vendor are included. Regulations, standards and guidelines are cited here only if they are thedirect source of a conformance criterion: otherwise, then they are listed in the Appendices (section 6.1, Reference Documents). To avoid redundant listings, any referenced document (with its URL) is only listed in the first relevant subsection: subsequent references are abbreviated and placed in footnotes. No regulations are cited as normative in cMHAFF, becausethey are realm-specific. NOTE: Legislation and regulations will vary between realms (locations) internationally and even within a country (e.g., states or provinces). Applicable regulations takeprecedence over cMHAFF when overlap or discrepancies exist. CMHAFF does not replace or override regulations of a realm.
- ***Implementation guidance***: Guidance for app developers is included. As applicable, the differential application of conformance criteria by type of app is discussed, referencing theexemplary use cases described previously.

1. Product Development and Support

Section Overview

Prior to marketing a mobile app, the developer has a responsibility to ensure it meets Realm-specific rules and **regulations**. Although cMHAFF does not have guidelines for all aspects of the software product life cycle, cMHAFF still recommends that the product development life cycle, for new apps and for upgrades to apps, ensure that requirements for functionality, reliability, performance, scalability, safety, compatibility, portability, and maintainability have been addressed, as well as any requirements that relate to aspects that include these items previously described above:

- Product Information for consumers (e.g., App Store descriptions, product disclosures)
- Security
- Privacy
- Permission to use device features
- Data Access
- Data Sharing
- Terms of Use, Conditions
- Product Development, including risk management, user-centered design, compliance with applicable regulations, functions (product description), reliability, performance, scalability, safety, compatibility, and portability.

The security and privacy of information used by the app needs to be considered throughout the development phases of the app. Functionality must support the intended use of the app for the target users and stakeholders. Thorough and iterative risk assessment and requirement analysis, testing, evidence collection, documentation, and configuration management ensures quality to satisfy the needs of the application's various stakeholders[8]. Assessing the **usability** of the app helpsensure the app's viability and adoption; testing must be population-relevant and demonstrate reasonable product usability (accessibility) by people with visual, auditory and motor disabilities within the intended target audience. Establishing a system of **customer support** enables product defects and usability issues to be surfaced in a systematic way and helps problems related to use ofthe app to be effectively resolved and the developer to continually deliver the intended use of the app.

Section/Id#: 11 Type: Function	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PDS.1.1 Header	**Regulatory Considerations**		NC	1
This section is about the compliance of apps to applicable regulations for the domains (realms, locales, environments) in which they are intended to be used. CMHAFF is designed as a framework that can be further constrained (profiled) for these domains and does not require conformance to any specific locale's regulations.			NC	2
1. The app SHALL be analyzed to determine if regulatory approval (following Realm-specific regulatory rules) is needed before the app is used by the general public.			NC	3
2. IF it is determined that realm-specific regulatory rule approval is required THEN the app SHALL not be presented for general public use until regulatory approval is obtained.			NC	4
3. The App SHOULD have measures to safeguard minors in accordance with applicable regulations.			C	5
Section/Id#: **Type:**	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
PDS.1.1 Reference	**Related Regulations and Standards**	PDS.1.1	NC	6

The documents listed below are overviews of the regulatory landscape, rather than specific regulations governing mobile health apps. Specific references are listed either following the conformance tables, or in the Appendix.

- **USA Federal Trade Commission Mobile Health Apps Interactive Tool** for guidance as to which federal laws apply. (https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health- apps-interactive-tool) All USA mobile app developers should consult this tool, which includes determining if the app is a regulated "medical device" according to the U.S. Food and Drug Administration (FDA), and if so, obtaining necessary pre-market approval.

Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps. (https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document- existing-eu-legal-framework-applicable-lifestyle-and)This broad guidance for the European Union, analogous to the USA FTC document. It is complemented by country-specific guidelines. In the EU, some mHealth apps may fall under the definition of a medical device and therefore may have to comply with the safety and performance requirements of Council Directive 93/42/EEC concerning medical devices (https://ec.europa.eu/growth/single-market/european- standards/harmonised-standards/medical-devices_en).

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#

PDS.1.1 Implementation Guidance	**Implementation Guidance**	PDS.1.1	NC	**7**

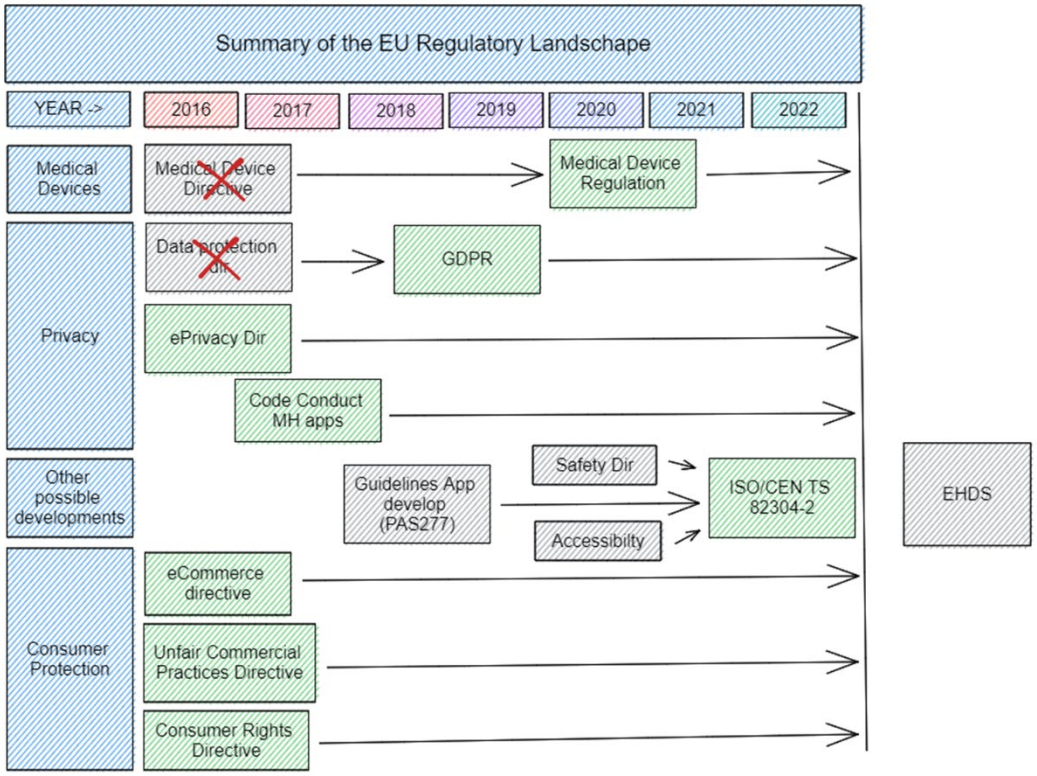
Implementation Guidance:

- Use Case A: In the US Realm, a walking app which encourages general wellness is not considered a mobile medical app by the FDA. As such the FDA does not intend to regulate this type of app.
- Use Case B: In the US Realm, a weight management app is not considered a mobile medical application by the FDA as long as it makes no claims to improve/cure a disease. How the app is described is important, and FDA guidance defining wellness vs. apps which aim to improve specific disease conditions should be referenced and reviewed before making a definitive decision as to its FDA classification.
- Use Case C: There are two distinctions regarding compliance issues for this app. For the data collection devices in this use case, a glucometer would be FDA regulated, while a general activity monitor, would not. Apps which collect and display disease information would not typically be regulated until the information is compiled or transformed and clinical decisions are made on the data. In this case, the app is capable of receiving alerts, but the logic behind the alerts are based on individualized settings through a rules engine which is integrated into an EHR. In this case, the locus of regulation is not clear, and as such counsel should be engaged in forming a definitive case as to what regulatory approvals might be needed.

For the European Union, the figure below summarizes relevant guidance and regulations for Mobile Health. There are three principal EU regulatory areas impacting mHealth apps:

- Medical devices, applying to higher medical risk apps only, including Regulation (EU) 2017/745 for medical devices in general and Regulation (EU) 2017/746 for in vitro diagnostic devices.
- Information protection, applying to all apps that store or transmit personal data – currently a group of three directives, that will largely be replaced by the General Data Protection Regulation on 25th May 2018, together with an expected mHealth-specific voluntary code.
- Consumer protection, including the right to fair treatment, products which meet acceptable standards, and right of redress if something goes wrong.

Shades of blue indicate directives and regulations. Red indicates voluntary codes/guidelines. Yellow indicates possible other actions with uncertain timing.



Section/Id#: Type:	**Header/Function Name** Conformance Criteria	**Reference**	**Chg Ind**	**Row#**
PDS.1.2 Function	**Product Risk Assessment and Mitigation**	PDS.1.2		8
	Statement: This category deals with process steps for risk assessment and mitigation for those who are developing a new app, or an upgrade to an app, prior to its being deployed to consumers. **Description:** Degrees of risk should be assessed and mitigated according to the intended use of the app. In general, risk management should manage security, privacy, safety, and other types of risks such as potential app failure scenarios, events that could lead to undesirable outcomes, probability and severity of risk, and mitigations or resolutions. One size does not fit all. For example, if apps handle sensitive personal information or give health interpretation or advice, higher degrees of risk are involved than for apps that do not collect personal information	PDS.1.2	C	9

or do not interpret or advise. If some information identified during this step should be disclosed to consumers, that is stated in the "Informing Consumers/Users" section.			
1. The App SHALL conform to a product risk assessment and mitigation plan as outlined by the developer. This plan should explicitly determine what risk must be addressed through software coding, hardware adaptions, policy, and what residual risk will be accepted by the entity responsible for the app. The developer will need to maintain, review, and update organizational Risk Register to include risks associated with mobile application.	PDS.1.2	C	10
2. In development of the App, the developer SHALL follow secure coding and practices using an established risk assessment framework.	PDS.1.2	NC	11
3. IF personally Identifiable Information is collected THEN in development the App SHALL be guided by risk assessment findings in terms of their potential effect on adequately securing an individual's personally identifiable information (PII) including any protected health information (PHI), and also information used to access an EHR/PHR (e.g., logon credentials).	PDS.1.2	C	12
4. IF the App transmits data to an EHR THEN the App SHALL document failure rates, measurement error rates, software bugs, and hardware risks of all types.	PDS.1.2	NC	13
5. Prior to product launch, the App SHOULD be approved in accordance with User Acceptance Testing (UAT) by testers who are not part of the formal development team.	PDS.1.2	NC	14
6. The App SHOULD be monitored and include documentation of conflicts or compatibility issues of the app with other apps, device features (e.g., camera), or connected devices.	PDS.1.2	NC	15
7. IF the App relies on external supporting infrastructure, (e.g., cloud-based servers) to operate, THEN the App SHOULD document measures to ensure the availability of that infrastructure.	PDS.1.2	NC	16
8. The App MAY provide documentation to show that the app publisher has adequate resources to continue to develop, maintain, and support the product (e.g., human resources, finances, IP rights, facilities, equipment, tools).	PDS.1.2	NC	17
Related Regulations and Standards	PDS.1.2	NC	18

While mobile computing environments may introduce some specific threats not present in non-mobilecomputing, the principles of risk management are the same across environments, so some standards and regulations are cited, even though they are not mobile-centric. Documents (listed alphabetically below) were sources of some cMHAFF criteria for risk assessment. Other useful references on risk assessment are listed in the Appendix. While some are realm-specific, they have much material that is applicable beyond their countries. Realms are listed in parentheses, if not explicit in the title.

Andalusian Complete list of recommendations on design, use and assessment of health apps:
http://www.calidadappsalud.com/en/listado-completo-recomendaciones-app-salud/

- **British Standards Institution Publicly Available Specification (PAS) 277:2015 Health and wellness apps – Quality criteria across the life cycle – Code of practice:** Recommendations andguidance throughout the app's product development life cycle
- **French Good Practice Guidelines on Health Apps and Smart Devices (Mobile Health or mHealth)**. https://www.has-sante.fr/portail/upload/docs/application/pdf/2017-03/dir1/good_practice_guidelines_on_health_apps_and_smart_devices_mobile_health_or_mh ealth.pdf
- **National Institute of Standards and Technology NISTIR 8144 Assessing Threats to MobileDevices & Infrastructure, *The Mobile Threat Catalogue*** (USA) https://nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf (context and background information)
  https://pages.nist.gov/mobile-threat-catalogue/application.html#vulnerable-applications (actual catalog of threats, specifically the "Vulnerable Application" category, which is the part ofthe threat catalog closest to cMHAFF)
- **Open Web Application Security Project (OWASP) Top 10 Mobile Security Risks:** https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10 This is focused on appdevelopers, so most of it is pertinent to cMHAFF, and for each risk, there are suggested mitigations.
- **OWASP Secure Coding Practices Quick Reference Guide:** https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/ - This provides resources for developers that can assist in implementing secure coding practices. It is recommended that developers adopt secure coding practices so that applications are developed with an emphasis on security vs having to apply security measures to protect the application.

Implementation Guidance	PDS.1.2	NC	19

While later sections in this standard include specific security and privacy controls to be applied to consumer mobile health apps, all products addressing health issues, regardless of their type, must be subjected to an overall risk analysis. This risk analysis may uncover the need for additional security controls over-and-above the conformance statements included in this document. As such, a risk analysis provides an additional layer of considerations such that conformance statements are not misused as a simple checklist in which it is assumed all security risks have been addressed if an app is in compliance with the conformance statements in this standard. For an app/product, the risk analysis should be conducted for the target environment(s) where the app will actually be used by consumers. Because of the diversity of consumers, such a risk analysis is wider ranging and more challenging than a risk analysis for the development organization's own environment.

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PDS.1.3 Function	**Usability/Accessibility Assessment**	PDS.1.3	NC	20

Statement: This category is about the assessment of usability during the product development cycle, for the intended use by a target audience.

Description: Certain accessibility requirements (usability for users with specific disabilities) are recommended, but the list is not exhaustive. Other

disabilities not mentioned (e.g., cognitive/learning disabilities) should be considered under the umbrella of conformance criterion #1.

1. The App SHALL be assessed against an industry-validated usability assessment tool, using subjects who are demographically similar to intended users (target audience). For example, user types may include those with motor disabilities, visual impairment, auditory disabilities, etc.	PDS.1.3	C	21
2. Non-functional testing of mobile app usability SHOULD be conducted to assesses an app's user-friendliness, performance reliability, and adherence to end-user expectations for the targeted consumer group.	PDS.1.3	NC	22
3. A written usability assessment plan, including known problems with product usability and mitigation plan, SHOULD be created. NOTE: for U.S. Realm when an app is sponsored by a HIPAA covered entity, the force of this criteria is elevated to "SHALL" with plans specifically addressing usability issues for people with visual and motor disabilities.	PDS.1.3	NC	23
4. The App SHOULD follow design/style guide standards established by the platform provider(s) for the app (e.g., Android, iOS).	PDS.1.3	NC	24
5. The App SHOULD avoid excessive data use, minimizing it as much as possible, warning users when high data usage occurs (e.g., downloads and updates).	PDS.1.3	NC	25
6. A requirement analysis SHOULD be executed describing the use cases (business scenarios) and intended users for the app's main functions.	PDS.1.3	C	26
7. The App SHOULD permit flexibility (adaptation) to the user's specific abilities, needs, or requirements.	PDS.1.3	NC	27
8. Information about accessibility characteristics in the app description and in contextual assistance sections of the app SHOULD be provided.		NC	28
Implementation Guidance	PDS.1.3	NC	29

The timing of implementation of usability findings can be indicated in functional profiles based on the severity of findings. At a minimum a usability assessment plan includes information about the timeframe under which remediation will occur.

These conformance statements apply to any type of app addressed in this standard. However, specific usability measures and remediation plans will differ based on app functionality, intended users, and app platform, and as such this standard does not discuss specific controls; instead, it speaks to a development process which encourages inclusion and end user satisfaction.

See Appendix: Reference Documents

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PDS.1.4 Function	Customer/Technical Support	PDS.1.4	NC	30
1. Information as to how to access customer support, and channels of support (e.g., voice, email, text, Twitter) SHALL clearly be stated within the app's Terms of Use and as a feature accessible from within the app.		PDS.1.4	NC	31
2. Customer support SHALL be accessible prior to establishing a user account (e.g., User can contact customer support with questions about the app's Privacy Policy or Terms of Use before making a decision to actively use the app).		PDS.1.4	NC	32
3. Customer support SHALL be provided in the language(s) in which the app is published.		PDS.1.4	NC	33
4. Within the app's Terms of Use, or in documentation available from within the app, any open source code library or code under copyright used to develop the app SHALL be given attribution.		PDS.1.4	NC	34
5. IF a Support request involves accessing, disclosing, or changing customer data, the identity of the customer, and the customer's data access rights, SHALL be verified before any disclosure or changing of customer data.		PDS.1.4	NC	35
6. Customer support queries SHOULD receive responses which directly address a stated problem or issue within two business days. A simple acknowledgement that a query has been received, without additional action, is insufficient.		PDS.1.4	NC	36
7. App consumers SHOULD be provided with aggregated satisfaction ratings relevant to customer support terms and conditions as appropriate.		PDS.1.4	NC	37
8. A FAQ resource where users can find answers to common questions SHOULD be provided.		PDS.1.4	NC	38

2. Product Implementation

Section Overview

Apps are frequently marketed and downloaded through platform-specific “app stores.” Before an app can be housed within an app store, it must meet requirements set by the app store host. The app store is one primary source of product information for consumers to decide whether they want to install the app. In some realms, apps may also be obtained through an app registry.

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PIM.2.1	Product Information	PIM.2.1	C	39

This category is about providing information about the product to consumers and also other parties (e.g., governments, consumer or provider organizations) who have interest in potential purchase, use, endorsement, or recommendation of apps. The experience of installing an app begins at an app store and completes on a user device. See also the Conditions and Agreements section of this specification for guidance regarding Conditions and Agreements that usually appear as part of the app store experience. cMHAFF does not specify exactly how or where product information is conveyed,

e.g., app store, web site, online help.				
PIM.2.1.1	General Information	PIM.2.1	C	40
1. The description of an app SHALL include the main functionality, the intended use, the intended (target) audience, and potential use of the user's personal data by the app.		PIM.2.1	NC	41
2. Screen shots of the app SHALL accurately depict the screens of the current version of the product.		PIM.2.1	NC	42
3. Product information SHALL be provided before the app is used by the consumer, to help consumers decide whether the app is suitable.		PIM.2.1	NC	43
4. The app description SHOULD clearly states the human languages the app supports.		PIM.2.1	NC	44
5. Information about the app publisher (persons/organizations) SHOULD be provided and provide mechanisms to communicate with the publishers.		PIM.2.1	NC	45
6. Disclosure SHOULD be provided about sources of funding and possible conflicts of interest for the app (e.g., app use could incent user to buy products or services from app publisher).		PIM.2.1	NC	46
PIM.2.1.2	Payment	PIM.2.1	C	47
1. The payment amount for the app, if any, SHALL be clearly noted according to app store rules.		PIM.2.1	NC	48
2. Apps which have required or optional payments after download SHALL clearly state this in their app store description, along with the amount of payment required and the actions which result from such in-app payments (for example, payment of a certain amount results in an ad-free experience when using the app). The impact of not making payments must also be stated (e.g., limited functionality).		PIM.2.1	NC	49
3. App users SHALL be notified if they are being signed up for a set period of recurring payments.		PIM 2.1	NC	50
PIM.2.1.3	Evidence/Credentials	PIM.2.1	C	51
1. IF the app provides health recommendations, the scientific degree of evidence and the types and dates of sources used (e.g., clinical practice guidelines and protocols, peer-reviewed articles, professionals and organizations with their credentials) that guided the app content SHALL be disclosed.		PIM.2.1	NC	52
2. The App SHOULD reference/provide sufficient information so that consumers can easily access evidence for review. This could include clinical, social, technical, and other domains of potential relevance.				53
3. IF there is human and/or automated interpretation of health-related content, the credentials of qualified health professionals SHALL be disclosed, and/or the algorithms and testing plans and reports SHALL be documented.		PIM.2.1	NC	54
4. The app descriptions SHOULD identify the health professionals and credentials of those who worked on the app and/or at least the professional organization that made, reviewed, endorsed, or sponsored the app.		PIM.2.1	NC	55
4. The date of the last update to the app SHOULD be shown and the changes from the previous release described (e.g., revisions due to new scientific evidence).		PIM.2.1	NC	56
5. The degree of admission of liability (publisher's acceptance or disclaimer of responsibility) regarding the selection and use of the app's content SHOULD be declared.		PIM.2.1	NC	57
6. The app description MAY include data related to app reliability and validity tests or population research results.		PIM.2.1	NC	58
PIM.2.1.4	Limitations and Warnings	PIM.2.1	C	59
1. Contraindications, potential risks and limitations of use SHALL be documented. For example, environmental or patient conditions under which apps or connected devices may be unreliable (e.g., tattoos that impact optical sensors; avoid usage when pregnant; avoid usage outside a temperature range).		PIM.2.1	NC	60
2. IF the app provides health recommendations (e.g., general guidelines) it SHALL disclose the potential risks to patient safety and their mitigations.		PIM.2.1	NC	61
3. IF the app collects de-identified data it SHOULD provide documentation as to how the data is de-identified and its current/planned secondary uses.				62
3. IF the app offers health advice (e.g., specific and personal health decision support)] it SHOULD be state that the use of the app does not replace the provider-patient relationship or the recommendation, opinion, or diagnosis of a health professional.		PIM.2.1	NC	63
5. Users SHOULD be warned of updates caused by possible errors in functionality, in health-related information, or in any other sensitive data.		PIM.2.1	NC	64
6. IF the app has collected personal health information, it SHALL guarantee the integrity of data stored across different versions of the app.		PIM.2.1	NC	65
PIM.2.1.5	Technical Details	PIM.2.1		66
1. IF the user can enter personal health information into the app, it SHALL clearly disclose whether or not data validity checking is done, and document or reference the evidence for such validity checking.		PIM.2.1	NC	67
2. IF the app collects or receives quantitative data, the precision (accuracy, granularity) of measurements (e.g., physical activity, physiological data from connected devices) SHALL be		PIM.2.1	NC	68

documented and justified as appropriate for the intended use of the app.			
3. IF personal health information is hosted, backup and recovery procedures SHALL be documented and compliant with applicable regulatory requirements.	PIM.2.1	NC	69
4. IF Personal health data are imported or exported, functions for data import or export SHALL be documented, including the ability to convert to standard formats.	PIM.2.1	NC	70

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PIM.2.2 Function	Launch App and Establish User Account	PIM.2.2	NC	71
1. A user SHALL be able to review the app's Terms of Use before personal data about the user is collected and used.		PIM.2.2	NC	72
2. IF the app creates user accounts, the user acceptance of the app's Terms of Use SHALL be logged before a user account is authorized (See section 3.4.10 for information about audit log record creation).		PIM.2.2	NC	73
3. IF the user is allowed to use pre-existing account credentials from an Identity Provider (IDP) to access the app, before a user chooses to use pre-existing account credentials to access the app: (a) The user SHALL be informed about what attribute information will be used by the app associated with the pre-existing credentials; (b) The user SHALL be informed about what data is communicated back to the IDP at the time of account creation and at each subsequent user authentication.		PIM.2.2	NC	74
4. For purposes of establishing an account, no more than the minimum necessary amount of a user's personally identifiable information (PII) SHOULD be collected, e.g., the information is necessary to authenticate the user, provide customer support, or affect the app logic.		PIM.2.2	NC	75
Implementation Guidance		PIM.2.2	NC	76

- Use Case A: Knowing who the user is, in an absolute sense, is not needed as data is not being sent to any external data set. Primarily, account controls are in place to ensure the same person is using the app each time. For this walking app, possession of a smartphone may be sufficient to allow someone to use it without any additional need for authentication or need to set up a unique user ID and password to access the app.
- Use Case B: Knowing the user's absolute identity is not needed but minimal account controls (e.g., user ID and password) should be established as the app will allow information to be sent to an existing data set, and these data sets will need some ability to be linked, in part showing evidence an individual has control over both the app data and a right to access the existing data set.
- Use Case C: requires more rigorous identity proofing as data will be both sent to an EHR and interactions initiated by a physician result in information being pushed to the app. Identity proofing can occur within the app itself, or in the use of pre-existing identity credentials (e.g., patient portal credentials for the entity controlling the EHR) to establish identity.

3. App Use

Statement Overview: This section addresses functionalities and considerations to be addressed while the user is operating the app.

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
APU.3.1 Function	Authentication	APU.3.1	NC	77

Statement: This category is about the system protecting against unauthorized access (e.g., by persons other than the consumer).

Description: The functionality of an app, its sponsorship, and linkages to external data sources all affect the security, privacy and data controls which are established to ensure safe and effective use. In this section, conformance criteria point to issues which can be addressed through a range of options, and as such implementers should consider not only the conformance criteria but the discussion regarding applicability to the exemplary use cases.

1. The identity of an app user SHALL be authenticated prior to any access of PHI or PII.	APU.3.1	NC	78
2. The method of authentication SHALL be communicated to the app user when an app account is established.	APU.3.1	NC	79
3. The app user SHALL be authorized to access a feature of the app before that feature or any associated PHI or PII is displayed. Authorization may be internal to the app or derived from an external source.	APU.3.1	NC	80
4.At the request of an app user, the app SHALL terminates such that access to PHI or PII requires a new, successful authentication attempt.	APU.3.1	NC	81
5. IF other external HIT system (e.g., EHR) is a system actor, a subject's association with their real-world identity SHALL be verified, establishing that a subject is who they claim to be (identity proofing).	APU.3.1	NC	82
6. IF the EHR is a system actor, the EHR SHALL authorizes an app user' access to app features when these features are supported by data provided by or written to the EHR.	APU.3.1	NC	83
7. IF PII or PHI are displayed, the app SHALL terminate the app or makes PHI or PII invisible after a period of time of user inactivity as described in the app's Terms of Use. This feature is sometimes called "inactivity timeout" "Session timeout" or "automatic logoff". The determination to include this feature within an app is made as part of the overall risk analysis regarding the sensitivity of data provided by or through the app.	APU.3.1	NC	84
8. IF passwords are stored on the device, passwords SHALL be encrypted and never displayed as plaintext.	APU.3.1	NC	85

	9. IF access to account exposes Protected Health Information (PHI) or PII, the user SHALL be given an option to utilize strong authentication methods (e.g., multi-factor authentication and/or biometrics) in addition to passwords. Before selection of this option, the mechanism for authentication is clearly described and/or demonstrated to the user. This capability may apply to an app itself, and also to the pairing of the app with a device.	APU.3.1	NC	86
Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
APU.3.2 Function	User Authorizations	APU.3.2	NC	87
	Statement: This category is about personal data collection and use, including access to device features, being understood and explicitly authorized (consented to) by the users of the app.			
	1. Smartphone functionality and data sources SHALL only be used when essential to perform specific functions of the app. This includes, but is not limited to, the use of: location services, camera, microphone, accelerometer and other sensors, contact lists, calendars.	APU.3.2	NC	88
	2. Before using select smartphone functions and data sources for the first time, app users SHALL be asked for permission to use these services and data sources. Permissions for each function, data source and user tracking activity controlled by the app can be individually specified by the user.	APU.3.2	NC	89
	3. Before exporting data from the smartphone, or from any device integrated with the smartphone, the app user SHALL be asked for permission to transmit the data with an explanation of what data is being transmitted, and to which recipients for what purposes (e.g., to servers of the app supplier, for backups, for big data analysis). Permission is requested before the first potential transmission of data. Permission is re-requested the first time any additional data elements are sent to an external data source when permission had previously been extended for a smaller set of data. Permission is not requested at every transmission, if the scope of exported data remains unchanged.	APU.3.2	NC	90
	4. IF the app requests permission to use data generated by the app after it is de-identified, the account holder SHALL be informed of who would have access to the de-identified data and for what purpose.	APU.3.2	NC	91
	5. IF the app requests permission to use data generated by the app after it is de-identified, the account holder SHALL be informed of the possibility that de-identified data can potentially be re-identified and steps the app sponsor takes to prevent re-identification.	APU.3.2	NC	92
	6. IF the user gives permission for data generated by the app to be de-identified and used, the data de-identification, at minimum, SHALL follow realm-specific rules (e.g., HIPAA safe-harbor in USA).	APU.3.2	NC	93
	7. IF in-app payments exist, the in-app payments SHALL not be triggered in such a way that can expose healthcare-related information to payment organizations.	APU.3.2	NC	94
	8. IF the app uses in-app advertising, potential use of PHI or PII to personalize advertisements from the app SHALL be disclosed to the user, who shall be given the opportunity to consent or decline.	APU.3.2	NC	95
	9. IF the app requests to share data with social networks, the app SHALL provide the user with options to select which types of data will be shared, and informed of potential consequences of the secondary use and sharing of that data outside the app's control. Only after consent from the user can data sharing commence with the social networks. 1]	APU.3.2	NC	96
	10. An app user can choose to permit some, but not all, requested data to be exported from a smartphone or associated device. The user SHOULD be informed as to how the choice to limit data affects the functionality of the app.	APU.3.2	NC	97
	11. IF an app user denies a permission requested by the app, the app users SHOULD be informed of the consequence of not extending the permission and is given a second chance to extend a permission.	APU.3.2	NC	98
Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
APU.3.3 Function	Pairing or Syncing User Accounts with Devices and Data Repositories	APU.3.3	NC	99
	Statement: This category is about consumer verification of all devices to which they wish to pair or sync data.			
	1. The App SHALL ensure that the user has successfully authenticated and has an active session before pairing an external device to an app account.	APU.3.3	NC	100
	2. Before a device is paired with an app to collect information about a specific individual, the app SHALL display a screen which asks the user to confirm that the device will collect information about a specific, named person. The person may be the account holder or a proxy subject of the account holder.	APU.3.3	NC	101
	3. The App SHALL provide a person who pairs a device with an individual in context of use of a specific app the ability to un-pair the device and individual through an app utility function.	APU.3.3	NC	102
	4. Before a device is paired with an app to collect information about a specific individual, the app SHALL state what data will be collected by the device and how the device data is used. This statement may include a link to an informational page which provides details about data collection and use.	APU.3.3	NC	103
	5. IF data for more than one person can be collected by the app/device pair the app SHALL ask the account holder to confirm the person for whom data will be collected by the device before data is collected and transmitted.	APU.3.3	NC	104

6. IF the developer includes a syncing option within the APP (e.g., same app data synchronized across smartphone and tablet devices)]. The app SHALL provide the user with the option to consent with syncing process.	APU.3.3	NC	105
Section/Id: Type: **Header/Function Name** Conformance Criteria	**Reference**	**Chg Ind**	**Row#**
APU.3.4 Function — Security for Data at Rest and in Transport	APU.3.4	C	106
Statement: This category is about providing assurance that the consumer's stored data is secure, regardless of whether it is stored on the consumer's devices or elsewhere (e.g., in cloud-based servers for an app). It also provides assurance that consumer data is secure when it is moved between the consumer's device(s) and other locations.			
1. The app SHALL be developed in a manner that ensures that PHI and PII stored on a smartphone is stored as encrypted values.	3.4	NC	107
2. The app SHALL be developed in a manner that ensures that PHI and PII stored by the mobile app on any external server is stored as encrypted values.	3.4	NC	108
3. The app SHALL ensure that unless PHI and PII has been transmitted to a data set maintained by a Health Plan or Health Provider, the account holder can delete information collected through the app, including data generated by a device associated with the app.	3.4	NC	109
4. The App SHALL improve and/or upgrade encryption cipher and suites to match evolving best practices when actively being developed and maintained (e.g., not currently being sun-setted).	3.4	NC	110
5. IF the app contains PHI and/or PII it SHALL be developed in a manner that ensures that PHI and PII data transmitted between an app and an external data source, including data generated through a device associated with the app, are transmitted as encrypted values.	3.4	NC	111
Section/Id: Type: **Header/Function Name** Conformance Criteria	**Reference**	**Chg Ind**	**Row#**
APU.3.5 Function — Data Authenticity, Provenance, and Associated Metadata	APU.3.5	NC	112
Statement: This category is about providing assurance that consumer data is secure when it is moved between the consumer's device(s) and other locations. This category is about the attribution of sources of data (provenance) and assurance of data authenticity.			
1. The app SHALL conform to Best Practices for Data Authenticity, Provenance, and Associated Metadata.	APU.3.5	NC	113
2. IF the App itself originates data <see ISO 21089 definition of originates>] the App SHALL provide the customer with the option to review, irreversibly destroy, reject or discard data.	APU.3.5	NC	114
3. If the app itself only receives data as a pass through and cannot store data the app SHALL provide the customer with the review option to display the data prior to executing the pass-through which includes the option to irreversibly stop and block the pass-through.	APU.3.5	NC	115
4. IF the app itself receives data and stores it then the app SHOULD provide the customer with a review option that permits only appending data and/or free text comments to received data as author while preserving the original received data intact with original provenance. User may comment that data are erroneous, but does not have the option to delete the original data.	APU.3.5	NC	116
Related Regulations and Standards	APU.3.5	NC	117

The following are examples of standards for data provenance. Even though they are specific to the FHIR and CDA standards respectively, the principles and data elements -- for recording entities and processes involved in producing or delivering a resource (data) – may be applicable.

- **FHIR Provenance Resource** http://www.hl7.org/FHIR/provenance.html
- **HL7 CDA® R2 Implementation Guide: Data Provenance, Release 1 - US Realm**

http://www.hl7.org/implement/standards/product_brief.cfm?product_id=420

- **ISO 21089 Health Informatics – Trusted End-to-End Information Flows.** https://www.iso.org/standard/35645.html Offers a guide to trusted end-to-end information flow for health(care) records and to the key trace points and audit events in the electronic entity/act record lifecycle (from point of record origination to each ultimate point of record access/use).

Section/Id: Type: **Header/Function Name** Conformance Criteria	**Reference**	**Chg Ind**	**Row#**
APU.3.6 Function — Data Exchange and Interoperability	APU.3.6	NC	118
Statement: This category applies only if an app exchanges data with other devices, health apps, and/or HIT systems. If so, there are applicable standards for data format, vocabulary, and transport, to increase interoperability and ease of connection.			
1. IF the App exchanges discrete clinical data, the app SHALL use standard terminologies (e.g., SNOMED CT, LOINC).	APU.3.6	NC	119
2. IF the app exchanges discrete clinical data, the app SHALL use standard format/content, e.g., HL7 FHIR, SMART on FHIR, HL7 Consolidated CDA, Detailed Clinical Models (HL7 CIMI), etc.	APU.3.6	NC	120
3. IF the App exchanges discrete clinical data with devices, the app SHOULD use standard format/content, e.g., IEEE 11073.	APU.3.6	NC	121
4. IF the app exchanges unstructured data, the app SHOULD use standard or commonly accepted formats, e.g., HL7 CDA, PDF.	APU.3.6	NC	122
5. IF the app collects personal health information, the app SHOULD allow data to be imported or exported from the app.	APU.3.6	NC	123

Related Regulations and Standards	APU.3.6	NC	124

- **Direct Project Applicability Statement for Secure Health Transport** https://www.healthit.gov/policy-researchers-implementers/direct-project
- **HL7 Consolidated CDA**
- **HL7 FHIR STU.** http://www.hl7.org/FHIR/index.html
- **SMART ON FHIR.** https://smarthealthit.org/
- http://www.hl7.org/implement/standards/product_brief.cfm?product_id=379
- **IEEE 10073 Personal Health Data Standards** https://standards.ieee.org/develop/wg/PHD.html
- **"MedMij" information Exchange standards for Personal Health Environment** https://www.medmij.nl **(**Netherlands) Includes HL7 Health Clinical Information models (HCIM), which provide context for discrete clinical data (e.g., systolic blood pressure); the standard is being used in the Netherlands.

Section/Id: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
APU.3.7 Function	Notifications and Alerts	APU.3.7	NC	125

Statement: This category applies only if an app exchanges data with other devices, health apps, and/or HIT systems. If so, there are applicable standards for data format, vocabulary, and transport, to increase interoperability and ease of connection.

1.The app SHALL require opt-in consent from the account holder before sending notifications and alerts.	APU.3.7	NC	126
2. The app SHALL inform the account holder of both the content and channel (SMS, push notification, email, etc.) of the notification or alert that is consented to.	APU.3.7	NC	127
3. The app SHALL provide the account holder with the ability to change consent decisions about notifications and alerts through settings available on the device on which the app was downloaded.	APU.3.7	NC	128
4. The app SHALL provide notifications and alerts that contain the least amount of information necessary for the recipient of the alert to take a focused action.	APU.3.7	NC	129
5. IF alerts notify the user of conditions that are abnormal, exceptional, or determined out of range, the App SHALL document or reference the sources (evidence base) of the formulas/algorithms upon which such alerts and notifications are based.	APU.3.7	C	130
6. IF permitted by the account holder and agreed to by recipients, the App SHOULD provide the ability to send notifications and alerts to the account holder and/or to another person or entity.	APU.3.7	NC	131
7. The App SHOULD provide alerts to notify the user of potential faults that could cause inconvenience or harm to the user, e.g., low battery alerts.	APU.3.7	NC	132
8. The App SHOULD notify the user in case of external interruptions or delays (e.g., loss of network connection, database problem, lengthy operation).	APU.3.7	NC	133
Implementation Guidance	APU.3.7	NC	134

In the realm of alerts and notifications, the following table proposed suggested standardized (generic)terms in the left column, with mappings to the leading two platforms in the middle columns, and comments in the right column. The platform-specific definitions have been derived from web sources,with preference given to information from the creators of the platforms (Apple, Google). Note: the mapping cannot be made an exact 1:1. In some cases, the platform-specific term may be more precise(e.g., subtypes) than the generic term, but we do not require a generic equivalent for every platform- specific term. In other cases, there may be substantial similarity of concepts across platforms, but not identical behavior, and certainly not identical appearance.

Despite the proposed granularity of these terms, that does not mean that there need to be separatecMHAFF conformance requirements for each type, but at least the opportunity is there if the need arises. In particular, there may be different conformance requirements for "alerts" vs other types ofnotifications.

Suggested "standardized" (generic) term for cMHAFF	Apple (iOS) equivalent	Google (Android OS) equivalent	Comments
Message Any computer to computer or computer-to-human interface, whether via visual, aural, haptic, olfactory, taste, or neural mediums. However, when discussing interoperability, the focus is on computer-to-computer[3] messaging. Note that the messages can be transmitted within the same physical computer, but between different software (e.g., APIs).	Generally refers to messages within specific types of apps, like email, text, IM, Facebook…	Generally used to refer to messages from one device (or server) to another.	Message, or Messaging, can describe cMHAFF's overarching term for the data packages that are sent by apps. While we consider notifications and alerts as special types of messages, the specific term "message" is used a lot for messages within apps, but not generally used when describing alerts and notifications. We in HL7 also have the HIT-specific legacy of structured "messaging" formats that include healthcare content and sometimes PHI (e.g., HL7 v2 message).
Notification A device-specific message communicated to a user to inform	Notification – generic term to cover many types of notifications.	Notification – generic term to cover many types of notifications.	Generic term that has subtypes. While HIT also has "notifications" that

them of device or app activities that are deemed important to the user. Some types of notifications require a response from the user, while others do not.			may be delivered to an app, not just to a human user, cMHAFF uses a common consumer-based definition
Alert A type of Notification that is communicated to a user and requires a response before the user can proceed with activity on the device. For example, it may take the form of a "modal" pop-up dialog that must be dismissed by clicking OK or taking some other action.	Alert	Alert Dialog, aka Dialog Notification	These messages will always be seen by the user, except if the device is turned off or the user does not look at the device at all (nothing is guaranteed). In general, these are considered more "serious" than other types of notifications. Local or other policy make have more stringent rules for anything deemed an "alert" vs a "notification."
Persistent Notification A device-specific message communicated to a user to inform them of device or app activities and remain displayed on the device. These remain persistent until the user deletes them or takes an action that changes their status (e.g., checks text messages, checks email)	Notifications (in Notification Center) Badge (on individual app icons)	Status Notification Status Notifications can appear outside the app window and can be used to attract the user back to the app.	Android has more than one type of notification.
Temporary Notification A subtype of Notification that does not remain displayed on the screen more than a short time period.	Banner "Lock screen notifications" look like banners but appear on the lock screen.	Toast Toasts appear within the app window, not outside of it	Since these messages fade after a short time, it is very possible that they will not be seen at all. In Android, Toasts appear within the app window (not outside the app). In iOS, they can appear outside the app.
Emergency Notification A notification from an external source, such as the government, communicating important information about your area (e.g., emergency, disaster, weather…)	iPhone provides options for two types of Government Alerts, "AMBER Alerts" and "Emergency Alerts."	Four types: presidential notifications, imminent extreme notifications, imminent severe alert and AMBER alert. You can turn off every alert except for the presidential alert.	These are outside the scope of an app, are not written by MH app developers, but can be configured to display on the device. They are mentioned so that we don't use the same terms for something else.

Hierarchy

- **Message** (overarching term)
  - **Content Message** (e.g., HL7 v2, C-CDA payload, FHIR resource) – out of the scope for this set of definitions.
  - **Notification** (overarching term)
    - **Alert** (**requires** user action, whereas all other types of notifications do not require it,though they may allow it)
    - Persistent notification
    - Temporary notification
    - **Emergency Notification** (government, outside app control)

Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
APU.3.8 Function	Product Upgrades	APU.3.8		135
1. The App SHALL respect operating system level permissions concerning automatic product updates.		APU.3.8	NC	136
2. IF an updated version of the app includes updated terms of use, the App SHALL present Updated Terms of Use to the account holder for acceptance before an updated version of an app may be used. Significant changes to terms and conditions are highlighted, and a link to the full set of updated Terms of Use is available.		APU.3.8	NC	137
3. IF automatic app updates are not enabled, the app SHALL prompt the user to the availability of a new version of the app when a new version is available.		APU.3.8	NC	138
4. IF an account holder elects to not install a new version of an app, the App SHALL inform the user of the consequences of not installing the new version of the app, including information about support limitations for the older version of the App.		APU.3.8	NC	139
5. IF the new version of app increases what information is exposed by alerts, the App SHALL require the user to consent to the information being exposed, and the changes to the exposed information must be clearly highlighted when they make that consent.		APU.3.8	NC	140
Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
APU.3.9 Function	Audit	APU.3.9	NC	141

Statement: This category is about auditing, which is a mechanism for user and system accountability. Important events, such as logins and access to particular functions and data, are recorded and can be used to detect instances of non-compliant behavior and to facilitate detection of improper creation, access, modification, and deletion of personal health information. Any information technology including consumer health apps should follow best practices in managing an audit trail. The audit trail should maintain a record of users who have accessed what data, from where, and when. Audit logs should also record any attempts to access the system from an unauthorized terminal; expired usernames or passwords that try to access the system, unusual numbers of authentication attempts, and violations of an organizations security policy.

1. IF user authentication is required to access the App, the App SHALL generate an audit record of authentication attempts, both successful and unsuccessful.	APU.3.9	NC	142
2. The App SHALL generate an audit record of user permissions to access, or the revocation of access, regarding smartphone/tablet device capabilities for use by the app (e.g., use of camera, location services).	APU.3.9	NC	143
3. IF the App uses external devices or data sources for data collection, the App SHALL generate an audit record of the pairing of a device or data repository external to the app, which supplies data used by the app.	APU.3.9	NC	144
4. IF the App allows for the export of data to a data repository external to the app, the App SHALL generate an audit record of any export of data from the app.	APU.3.9	NC	145
Related Regulations and Standards	APU.3.9	NC	146
• **Integrating the Healthcare Enterprise (IHE) Audit Trail and Node Authentication (ATNA) Integration Profile.** https://www.ihe.net/Technical_Frameworks/#IT This IHE profile references the **Internet Engineering Task Force (IETF) RFC 3881 Audit Record standard https://datatracker.ietf.org/doc/rfc3881/** • **HL7 EHR Records Management and Evidentiary Support Functional Profile, Release 1 (RMES)** (http://www.hl7.org/implement/standards/product_brief.cfm?product_id=86 **)** Provides functions in an EHR system that can help an organization maintain a legal record for business and disclosure purposes.			147
Implementation Guidance	APU.3.9	NC	148

Every consumer mobile health app needs an audit strategy, which includes what data will be generated for audit, who will be able to access audit records, the location where audit data is stored, the length of time audit information will be stored, and any ability to delete audit data. Audit for security events is highly dependent on the nature of the app itself; audit requirements will differ significantly based on app sponsorship (e.g., sponsor is a HIPAA entity or a commercial non-covered entity), the need for user authentication, and if data generated through an app is accessible by consumers, clinicians, or both.

Section/Id: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
AST.4.0 Header	App Service Termination	AST.4.0	C	149

Statement: Health apps may be used indefinitely or for a finite period of time and will consequently require the ability to terminate services with the app.

Description: Disuse may happen when a health condition improves, a new health habit is established, when motivation to use the app wanes, or when the user determines a different app better meets their needs. Procedures for how data continues to be retained and used after account closure must be clear and understandable and give the app user options for relocation of their data to a new data repository.

Section/Id: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
AST.4.1 Function	App and Data Removal	AST.4.1	NC	150
1. The App SHALL provide an account holder the ability to remove an app from a mobile device at any time.		AST.4.1	NC	151
2. The App SHALL inform the account holder of the consequences of removing the app (e.g., loss of locally-stored data) from a smartphone and given an opportunity to confirm the removal of the app before the app is removed.		AST.4.1	NC	152
3. The App SHALL provide the account holder with the ability to close an associated account or data store associated with the app.		AST.4.1	NC	153
4. The App SHALL inform the account holder of the consequences of deleting the account and given an opportunity to confirm closing the account before it is closed.		AST.4.1	NC	154
5. The App SHALL inform the account holder that data that was part of the account may have been transmitted to other systems, outside of the account itself, and may persist. For example, suppose the user collects device data in an app, and transmits that data to an EHR which stores it as PGHD. In this case, the user shall be informed that deleting the account may not delete the data that is now in the EHR.		AST.4.1	NC	155
6. The App SHOULD, before closing an app account, provide the account holder with the ability to download data generated by the account holder or a proxy subject of the account holder to a data set under the full control of the account holder (data portability).		AST.4.1	NC	156
7. IF the device that the App is installed on permits remote or external access to device data, the App SHALL provide the ability for any PHI or PII stored on a device to be wiped remotely by the account holder without deleting the account which is related to the wiped data.		AST.4.1	NC	157
8. The App SHOULD provide clear criteria that is set and communicated to the user regarding the deletion of data, including automatic deletion if the user has not used the App for a specified		AST.4.1	NC	158

period.				
Related Regulations and Standards		AST.4.1	NC	159
• **European Union Privacy Code of Conduct on Mobile Health apps** https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps				160
Implementation Guidance		AST.4.1	NC	161
Data download should be in a standard or at least nonproprietary format (e.g., CSV, XML, JSON) that can be manipulated by off-the-shelf tooling. The format should be selected appropriate to the data being downloaded.				162
Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
PUD.4.2 Function	Permitted Uses of Data Post Account Closure	PUD.4.2		163
Statement: This category is about what is done with consumers' data if they close their account (terminate use of the app).				
1. The App SHALL not disclose data associated with a closed app account to any new persons or entities. This includes data which has been de-identified.		PUD.4.2	NC	164
2. The App SHALL offer the consumer the option to decide what to do with their data (keep, delete, etc.).		PUD.4.2	NC	165
Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
CNA.5.0 Header	Conditions and Agreements	CNA.5.0	NC	166
Statement: This section of cMHAFF deals with nonfunctional, and usually nontechnical, aspects of mobile health apps. While not traditionally in scope for HIT standards oriented at large or small enterprise organizations, it is a very important and distinctive characteristic of apps targeted at consumers. **Description:** Since one goal of cMHAFF is consumer protection, including their privacy and security, guidance in the area of "Conditions and Agreements" (CnA) is offered. CnA is not a formal or legal term, but an umbrella under which can be grouped various expressions of conditions that consumers to which are asked to agree before they start using a mobile health app. These may be called "Terms and Conditions," "Terms of Use," "Terms of Service," "End User License Agreement (EULA)," and similar concepts. Typically, CnA are displayed and consumers are asked to click buttons to agree to terms, when they interact with "App Stores" (a generic term including wherever a consumer downloads a mobile health app). In addition to what the consumer agrees to, CnA may also commit the app supplier to certain behaviors or restrictions. While cMHAFF does not prescribe what these CnA must include, it provides guidance as to items that are important to disclose. In that respect, there is some precedent in the ONC 2015 Edition Certification, which contains disclosure and transparency requirements for EHR developers, e.g., about pricing and services that are not included in the base software.				
Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
CNA.5.1 Function	Specifications for Conditions and Agreements	CNA.5.1	C	167
1. The App developer SHALL, before download, allow the potential user to easily access the Apps Terms of Use. This may be accomplished through a link in the app description in the relevant app store.		CNA.5.1	C	168
2. The App developer SHALL, before download, allow a potential user to easily access the App's Privacy Policy. This may be accomplished through a link in the app description in the app store.		CNA.5.1	NC	169
3. IF rewards are given for app participation, the App SHALL clearly disclose all conditions and time limitations governing rewards. These include but are not limited to: how activity is tracked; how promptly rewards are fulfilled; whether rewards can expire or be withdrawn; whether and how rewards can be transferred to another person; whether rewards can be accumulated into larger rewards; etc.		CNA.5.1	NC	170
4. The App SHOULD provide the ability for the consumer to indicate that they acknowledge and understand the app functionality.		CNA.5.1	NC	171
5. IF the App includes in-app payments, the App SHALL provide a disclosure of what is included as base functionality without payment, and what functionality would require additional payment.		CNA.5.1	NC	172
6. IF the App permits in-app payments, the App SHALL clearly state the benefits for paying for a service or feature in a manner which allows an account holder to make an informed decision about making or declining an in-app payment.		CNA.5.1	NC	173
7. IF App access is by subscription, the App SHALL clearly state the requirements for cancelling a subscription in the CnA.		CNA.5.1	NC	174
8. IF the App requires an additional charge to upgrade, the App SHALL clearly state in the CnA the upgrade charges, the amount of advance warning for upgrades, and the length of support for the old version (if not upgraded).		CNA.5.1	NC	175
9. The App SHALL disclose the use of advertising mechanisms, distinguish advertisements from app content, and provide ways to deactivate or skip advertisements.		CNA.5.1	NC	6
10. The App SHOULD provide a means for a user to access the App's Privacy Policy at any time during the usage of the app.		CNA.5.1	NC	177

Related Regulations and Standards	5.1	NC	178
• **Federal Trade Commission: How to Make Disclosures in Digital Advertising, March 2013** *https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf* (USA). Explains how to make disclosures clear and conspicuous to avoid deception and takes into account the expanding use of smartphones. •			179

Section/Id: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
DEF.6.0 Definition	Definitions (Glossary)	DEF.6.0	NC	180

Statement: Philosophically, the Mobile Health workgroup favors using terms that are commonly accepted in the consumer mobile space, in preference to terms that are used only in the EHR space, because of the target user for these devices, who are consumers rather than clinicians. However, where terms are used differently in EHR vs consumer spaces, we take note of that, and acknowledge the various uses. This does not purport to be an exhaustive set of mobile health definitions, but terms are included only to provide clarity within cMHAFF. See **British Standards Institution Publicly Available Specification (PAS) 277:2015 Health and wellness apps. Quality criteria across the life cycle. Code of practice** (https://shop.bsigroup.com/products/health-and-wellness-apps-quality-criteria-across-the-life-cycle-code-of-practice) which has a good set of Terms and Definitions (section 3). Definitions below that are taken from PAS277 are labeled (PAS).

Term	Definition
Alert	A type of message that conveys information that is important enough to require a user response.
App	A software application that can be executed (run) on a computing platformand is typically a small application run or accessed on mobile devices. (PAS) Apps provide a specific set of functions which, by definition, do not include the running of the computer itself. In the context of cMHAFF, an app is the program that is downloaded to run on the user's device. It may be supported by additional infrastructure (such as cloud-based resources) for processing, storage, etc.
App store	A type of digital distribution platform for computer software, often in a mobile context. Also known as "app marketplace."
Assessment	In the context of cMHAFF, "assessment" is a broad term to describe evaluations of a consumer mobile health app based on the cMHAFF criteria. Assessment methods may range from self-attestation by an app publisher, through higher levels of rigor including testing, endorsement bya third party, and/or certification by an accredited body (with or without regulatory mandates). CMHAFF does not prescribe which method(s)should be used.
Caregiver	A caregiver is typically an unpaid or paid member of a person's social network who helps them with their health needs, often to address impairments related to old age, disability, a disease, or a mental disorder.For cMHAFF purposes, a caregiver *may* use a health app to help a person other than him/herself.
Consumer	A person who purchases goods or services for personal use. Specifically, for cMHAFF, the consumer is the acquirer of the mobile app.
Consumer mobile health app	An app intended to be used by a consumer (who may or may not be a "patient") rather than by a health professional. According to the US FDA:[25] "Mobile apps are software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach toa smartphone or other mobile communication devices, or a combination of accessories and software. Mobile *medical* apps are medical devices thatare mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device. Consumers can use both mobile medical apps and mobile apps to manage their own health and wellness, such as to monitor their caloric intake for healthy weight maintenance."
Detailed Clinical Model	A Detailed Clinical Model (DCM) is an information model of a discrete setof precise clinical knowledge which can be used in a variety of contexts. (http://wiki.hl7.org/index.php?title=Detailed_Clinical_Models)
Developer (app)	The person(s) or group(s) that technically developed (programmed) the app, which may be the same or different from the app Publisher orSponsor.
Directive (EU)	A directive is a legal act of the European Union which requires member states to achieve a particular result without dictating the means of achieving that result. It can be distinguished from **regulations** which are self-executing and do not require any implementing measures.

EHR	Electronic Health Record. An electronic version of a patient's health/medical history, that is maintained by the **provider** over time, andmay include all of the key administrative clinical data relevant to that person' care under a particular provider, including demographics, progress notes, problems, medications, etc.
FDA	Food and Drug Administration (FDA), a USA governmental agency whose regulations include medical devices and software as a medical device technologies. References may include: https://www.fda.gov/about-fda/what-we-do or https://www.fda.gov/about-fda/fda-organization/center-devices-and-radiological-health
Health and wellness app	An app that contributes to any aspect of the physical, mental or social wellbeing of the user or any other subject of care or wellbeing (PAS).
HIPAA	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and securityof certain health information.1 To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form.
Mobile medical app	Mobile apps are software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach toa smartphone or other mobile communication devices, or a combination of accessories and software. (see footnote 26)
Mobile platform	Commercial or open computing platforms, with or without wireless connectivity, that are hand held in nature (PAS). Typically, this includes smartphones, tablets, and wearables such as smart watches.
Notification	A general term for messages that convey information to a user. Alerts are a subset of Notifications: non-alert notifications convey information but do not require a user response.
Pairing	Pairing is establishing a trusted connection between two devices, e.g., ameasurement device such as a fitness tracker paired to a mobile phone.This is similar to how headsets or car audio systems are paired via Bluetooth to a mobile phone.
Personal data	Any information relating to an identified or identifiable natural person (PAS).
PGHD	Patient-Generated Health Data. Health-related data created, recorded, orgathered by or from patients (or family members or other caregivers) to help address a health concern. PGHD are distinct from data generated in clinical settings and through encounters with providers in two important ways: Patients, not providers, are primarily responsible for capturing or recording these data. Patients decide how to share or distribute these data to health care providers and others.
PHR	Personal Health Record, also known in some locales as a "Personal HealthEnvironment," is an electronic application used by **patients** to maintain and manage their own health information, and access to the information, in a private, secure, and confidential environment.
Publisher (app)	Individual or organization who is responsible for making the app available to users (PAS).
Sponsor (app)	Individual or entity who organizes and is committed to the development oruse of an app, e.g., a healthcare organization that sponsors an app for use by its patients, or an employer that sponsors an app for use by itsemployees.
Subject of care or wellbeing	Person whose care or wellbeing is being supported by use of the app (PAS).
Syncing	Syncing (synchronizing) is updating one or more devices to contain the same information, such as versions of an app, or data used by an app. Thisis similar to how a phone, tablet, and watch could share the same contact list.
User	Person who is directly using the app interface. Note that this may be the subject of care or wellbeing directly, or an individual assisting (as proxy for) the subject of care or wellbeing. An appmay have one or more subjects of care or wellbeing interacting with the same device, either under the same subject of care or wellbeing accountor using individual subject of care or wellbeing accounts. Each user may have one or more proxy users, either under the same user account or individual user accounts (PAS).

Section/Id: Type:	**Header/Function Name** Conformance Criteria	Reference	Chg Ind	Row#

REF.7.0 Reference	Appendices and Reference Documentation	REF.7.0	C	181

Statement: Outlined within this section are the numerous references and links to source documentation that have helped guide and inform development of the CMHAFF standard. This includes references to:

- The three pilots conducted in relation to HL7 CMHAFF STU 1 that helped inform the most recent cycle
- Links to guidance and documentation that informs unique implementation of CMHAFF depending on the goals and objectives of the health app under development
- Draft documentation on development of CMHAFF Labeling options for informing consumers of the quality/safety/privacy/security of a particular app based on review

Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
REF.7.1 Pilots	CMHAFF Pilots	REF.7.1	N	182

Three pilots were conducted in relation to the CMHAFF STU:

- Children's Hospital of Philadelphia
- Health App Analyzer– HRSA HITEQ
- CEN/ISO Health & Wellness Apps

Pilot Documentation: https://confluence.hl7.org/display/MH/cMHAFF+Pilot+Implementations

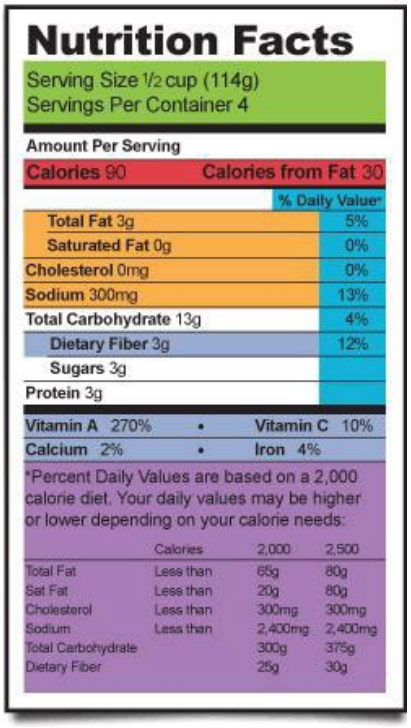
Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
REF.7.2 Reference	Reference Documents		C	183

Document	**Relevance to CMHAFF**
ONC API Task Force Final Report, https://www.healthit.gov/facas/sites/faca/files/HITJC_APITF_Recommendations.pdf	General, Authentication, Authorization
ONC Model Privacy Notice (updated December, 2016) https://www.healthit.gov/sites/default/files/2016_model_privacy_notice.pdf	Authorization for Data Collection and Use
Open Web Application Security Project (OWASP) Top 10 Mobile Security Risks: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10	Risk Assessment and Mitigation, Authentication, Authorization, Securityfor Data at Rest, Security for Data in Transit
U.S. Department of Health and Human Services, Usability Guidelines, U.S. Dept. of Health and Human Services. The Research-Based Web Design & Usability Guidelines, Enlarged/Expanded edition. Washington: U.S. Government Printing Office, 2006. https://www.usability.gov/sites/default/files/documents/guidelines_book.pdf	Usability
US Department of Health and Human Services (HHS) Summary of the HIPAA PrivacyRule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/ which includes a definition of PHI (also known as "individually identifiable health information") for the US realm.	Launch App and Establish User Account
U.S. Federal Trade Commission, Children's Online Privacy Protection Rule (COPPA), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa- frequently-asked-questions for the US realm. National Institute of Standards and Technology, Electronic Authentication Guideline, NIST 800-63-2.	Launch App and Establish User Account
U.S. Food and Drug Administration. Applying Human Factors and Usability Engineering to Medical Devices. February, 2016. https://www.fda.gov/downloads/MedicalDevices/.../UCM259760.pdf	Usability
U.S. Food and Drug Administration: Device Software Functions Including Mobile Medical Applications https://www.fda.gov/medical-devices/digital-health-center-excellence/device-software-functions-including-mobile-medical-applications. FDA Policy for Device Software Functions and Mobile Medical Applications, updated 9/26/2019 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications	Regulatory Considerations
U.S. Food and Drug Administration (FDA) – FDASIA Health IT Report. https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf	Risk Assessment andMitigation
U.S. Food and Drug Administration: Cybersecurity https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity	Risk Assessment and Mitigation
U.S. Food and Drug Administration (FDA) Digital Health Innovation Action Plan, https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf Indicates where FDA will and will not focus its regulations of mobile health apps.	Regulatory Considerations
W3C User Agent Accessibility Guidelines (UAAG) Overview https://www.w3.org/WAI/intro/uaag.php W3C Mobile Accessibility: How WCAG 2.0 and Other W3C/WAI Guidelines Apply to Mobile http://www.w3.org/TR/mobile-accessibility-mapping/	Usability
W3C Mobile Usability, http://www.w3.org/WAI/mobile/	Usability

Web Content Accessibility Guidelines (WCAG) 2.0, https://www.w3.org/TR/WCAG20/		Usability		
Section/Id: Type:	**Header/Function Name** **Conformance Criteria**	**Reference**	**Chg Ind**	**Row#**
Ref.7.3 Label		Ref.7.3	NC	184

It is possible that cMHAFF can assist both consumers (purchasers, users) of MH apps, as well as assessment organizations, through a "Label" that summarizes the major facts about the product. Well known examples (shown below) include Nutrition Facts labels and OTC Drug Facts labels required by governmental agencies. 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 bythird party testing (e.g., technical requirements for interoperability, security, etc.).

To be understandable, the Label should present cMHAFF categories in consumer-friendly language, notthe developer-centric terms used for the cMHAFF categories.



Nutrition Facts

Serving Size ½ cup (114g)
Servings Per Container 4

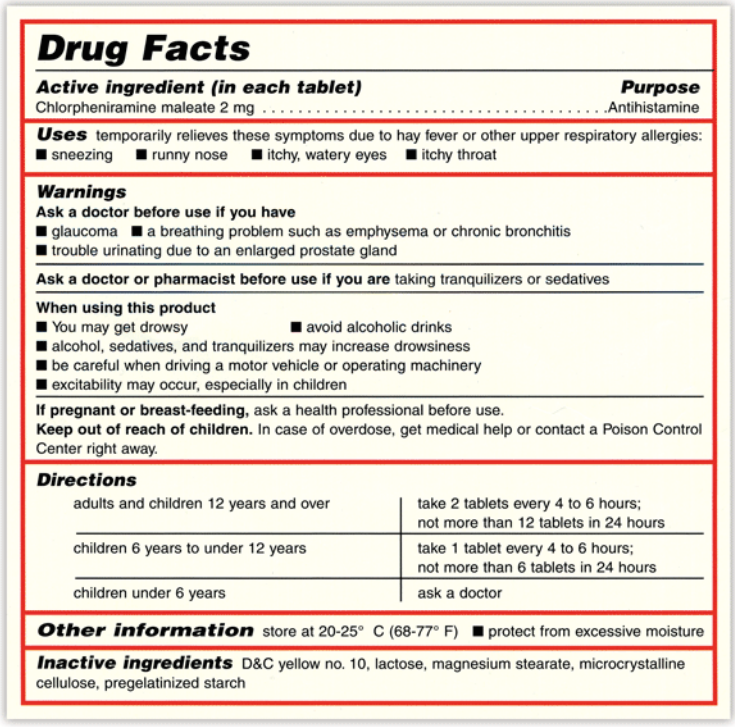
Amount Per Serving

Calories 90	Calories from Fat 30
	% Daily Value*
Total Fat 3g	5%
Saturated Fat 0g	0%
Cholesterol 0mg	0%
Sodium 300mg	13%
Total Carbohydrate 13g	4%
Dietary Fiber 3g	12%
Sugars 3g	
Protein 3g	

Vitamin A 270% • Vitamin C 10%
Calcium 2% • Iron 4%

*Percent Daily Values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs:

	Calories	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	80g
Cholesterol	Less than	300mg	300mg
Sodium	Less than	2,400mg	2,400mg
Total Carbohydrate		300g	375g
Dietary Fiber		25g	30g



Drug Facts

Active ingredient (in each tablet) **Purpose**
Chlorpheniramine maleate 2 mg ..... Antihistamine

Uses temporarily relieves these symptoms due to hay fever or other upper respiratory allergies:
■ sneezing ■ runny nose ■ itchy, watery eyes ■ itchy throat

Warnings
Ask a doctor before use if you have
■ glaucoma ■ a breathing problem such as emphysema or chronic bronchitis
■ trouble urinating due to an enlarged prostate gland

Ask a doctor or pharmacist before use if you are taking tranquilizers or sedatives

When using this product
■ You may get drowsy ■ avoid alcoholic drinks
■ alcohol, sedatives, and tranquilizers may increase drowsiness
■ be careful when driving a motor vehicle or operating machinery
■ excitability may occur, especially in children

If pregnant or breast-feeding, ask a health professional before use.
Keep out of reach of children. In case of overdose, get medical help or contact a Poison Control Center right away.

Directions

adults and children 12 years and over	take 2 tablets every 4 to 6 hours; not more than 12 tablets in 24 hours
children 6 years to under 12 years	take 1 tablet every 4 to 6 hours; not more than 6 tablets in 24 hours
children under 6 years	ask a doctor

Other information store at 20-25° C (68-77° F) ■ protect from excessive moisture

Inactive ingredients D&C yellow no. 10, lactose, magnesium stearate, microcrystalline cellulose, pregelatinized starch

Proposed cMHAFF Information Label for an App

The "Ind" column is an indicator (score) for the category, summarized by a color and a graphical symbol (green/up arrow = pass, red/down arrow=fail, yellow/side arrow=middle/partial). For "not applicable, cells are shaded gray and **…** is proposed as a graphical symbol.
SIMPLIFIED cMHAFF LABEL (LUMPING OF CATEGORIES)

App Name:		**Publisher:**
Category	**Ind**	**Other Contents (examples)[27]**
1. Product Information	□	Missing information on authors of app and evidence for app claims
2. Starting an Account	□	
3. Security and Trust	□	
4. Exchanging or Sharing Data	…	App does not share data
5. Ongoing Support and Updates	□	
6. Notifications and Alerts	□	
7. Ending Use of the App	□	Does not ask user about keeping or deleting data.
8. Product Development Process	□	"Follows all applicable laws recommended by FTC Mobile Health Tool"

Other icons, as alternatives to up/down arrows, include  or  The goal is to be internationally recognizable unlike letters, the meaning of which may be locale-specific.

Notes on Categories and Potential Assessment Methods

The category name is listed first (followed by the corresponding cMHAFF section names in parentheses). Then there is a consumer-friendly explanation of what that section includes, and finally a recommended means of assessment.
Principles of assessment:

- Green = all SHALL and SHALL [IF] statements met (where the [IF] conditions apply), plus some "subset of SHOULD criteria" (to be determined: may be some specific set of criteria, or some percentage).
- Yellow = Not all of the "subset of SHOULD criteria" were met. (This is the fuzziest area. It is "clean" if *all* SHOULD criteria are required for green, but that may be too tough)
- Red = one or more SHALL or applicable SHALL [IF] statements were not met

Notes on how measured (self-attestation, test, inspection, etc.).