HL7 Mobile Health Application Functional Framework; Consumer MHaFF, Release 1 (PI ID: 1182)



HL7 Mobile Health Application Functional Framework; Consumer MHaFF, Release x

DRAFT August 11, 2017

HL7 Informative Ballot

Sponsored by:
HL7 Mobile Health Work Group

Co-Sponsored by: HL7 EHR Work Group

Copyright © 2017 Health Level Seven International ® ALL RIGHTS RESERVED. The reproduction of this material in any form is strictly forbidden without the written permission of the publisher. HL7 and Health Level Seven are registered trademarks of Health Level Seven International. Reg. U.S. Pat & TM Off**.**

Use of this material is governed by HL7's [IP Compliance Policy](http://www.hl7.org/legal/ippolicy.cfm?ref=nav).

**IMPORTANT NOTES:**

HL7 licenses its standards and select IP free of charge. **If you did not acquire a free license from HL7 for this document,** you are not authorized to access or make any use of it. To obtain a free license, please visit http://www.HL7.org/implement/standards/index.cfm.

**If you are the individual that obtained the license for this HL7 Standard, specification or other freely licensed work (in each and every instance "Specified Material")**, the following describes the permitted uses of the Material.

**A. HL7 INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS,** who register and agree to the terms of HL7’s license, are authorized, without additional charge, to read, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part without paying license fees to HL7.

INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS wishing to incorporate additional items of Special Material in whole or part, into products and services, or to enjoy additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS as noted below, must become ORGANIZATIONAL MEMBERS of HL7.

**B. HL7 ORGANIZATION MEMBERS,** who register and agree to the terms of HL7's License, are authorized, without additional charge, on a perpetual (except as provided for in the full license terms governing the Material), non-exclusive and worldwide basis, the right to (a) download, copy (for internal purposes only) and share this Material with your employees and consultants for study purposes, and (b) utilize the Material for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, Compliant Products, in all cases subject to the conditions set forth in this Agreement and any relevant patent and other intellectual property rights of third parties (which may include members of HL7). No other license, sublicense, or other rights of any kind are granted under this Agreement.

**C. NON-MEMBERS,** who register and agree to the terms of HL7’s IP policy for Specified Material, are authorized, without additional charge, to read and use the Specified Material for evaluating whether to implement, or in implementing, the Specified Material, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part.

NON-MEMBERS wishing to incorporate additional items of Specified Material in whole or part, into products and services, or to enjoy the additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS, as noted above, must become ORGANIZATIONAL MEMBERS of HL7.

Please see http://www.HL7.org/legal/ippolicy.cfm for the full license terms governing the Material.

**Ownership. Licensee agrees and acknowledges that HL7 owns all right, title, and interest, in and to the Materials. Licensee shall take no action contrary to, or inconsistent with, the foregoing.**

**Licensee agrees and acknowledges that HL7 may not own all right, title, and interest, in and to the Materials and that the Materials may contain and/or reference intellectual property owned by third parties (“Third Party IP”). Acceptance of these License Terms does not grant Licensee any rights with respect to Third Party IP. Licensee alone is responsible for identifying and obtaining any necessary licenses or authorizations to utilize Third Party IP in connection with the Materials or otherwise. Any actions, claims or suits brought by a third party resulting from a breach of any Third Party IP right by the Licensee remains the Licensee’s liability.**

**Ownership. Licensee agrees and acknowledges that HL7 owns all right, title, and interest, in and to the Materials. Licensee shall take no action contrary to, or inconsistent with, the foregoing.**

**Licensee agrees and acknowledges that HL7 may not own all right, title, and interest, in and to the Materials and that the Materials** may contain and/or reference intellectual property owned by third parties (“Third Party IP”). Acceptance of these License Terms does not grant Licensee any rights with respect to Third Party IP. Licensee alone is responsible for identifying and obtaining any necessary licenses or authorizations to utilize Third Party IP in connection with the Materials or otherwise. Any actions, claims or suits brought by a third party resulting from a breach of any Third Party IP right by the Licensee remains the Licensee’s liability.

Following is a non-exhaustive list of third-party terminologies that may require a separate license:

| **Terminology** | **Owner/Contact** |
| --- | --- |
| Current Procedures Terminology (CPT) code set | American Medical Associationhttp://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/cpt/cpt-products-services/licensing.page? |
| SNOMED CT | International Healthcare Terminology Standards Development Organization (IHTSDO) <http://www.ihtsdo.org/snomed-ct/get-snomed-ct> or info@ihtsdo.org |
| Logical Observation Identifiers Names & Codes (LOINC) | Regenstrief Institute |
| International Classification of Diseases (ICD) codes | World Health Organization (WHO) |
| NUCC Health Care Provider Taxonomy code set | American Medical Association. Please see 222.nucc.org. AMA licensing contact: 312-464-5022 (AMA IP services) |

Contents

[1 Introduction 6](#_Toc490210714)

[1.1 Acknowledgements 6](#_Toc490210715)

[1.2 Background 6](#_Toc490210716)

[1.3 Intended Audience 6](#_Toc490210717)

[1.4 How to Use this Guide 6](#_Toc490210718)

[2 Overview 11](#_Toc490210719)

[2.1 Goals 11](#_Toc490210720)

[2.2 Scope 11](#_Toc490210723)

[2.2.1 In Scope 11](#_Toc490210724)

[2.2.2 Out of Scope 12](#_Toc490210729)

[2.3 Conformance Design Principles 13](#_Toc490210730)

[2.4 Exemplary Use Cases 13](#_Toc490210731)

[2.4.1 Use Case A: Simple, Standalone 14](#_Toc490210732)

[2.4.2 Use Case B: Device-Connected Wellness App 15](#_Toc490210733)

[2.4.3 Use Case C: EHR-Integrated Disease Management App 17](#_Toc490210734)

[2.4.4 Risk factors 18](#_Toc490210735)

[2.4.5 Summary of Major Differences in Use Case Scenarios 19](#_Toc490210736)

[2.5 Environmental Scan 19](#_Toc490210737)

[3 Conformance Criteria, Resources, and Implementation Guidance 21](#_Toc490210738)

[3.1 General Considerations 21](#_Toc490210739)

[3.2 Product Development and Support 21](#_Toc490210743)

[3.2.1 Regulatory Considerations 21](#_Toc490210750)

[3.2.2 Product Risk Assessment and Mitigation 23](#_Toc490210751)

[3.2.3 Product Usability 24](#_Toc490210752)

[3.2.4 CUSTOMER/TECHNICAL SUPPORT 25](#_Toc490210753)

[3.3 Download and Install App 27](#_Toc490210754)

[3.3.1 Informing Consumers/Users 27](#_Toc490210755)

[3.3.2 Launch App and Establish User Account 29](#_Toc490210756)

[3.4 Use App 31](#_Toc490210757)

[3.4.1 User Authentication and Authorization to Access App Services 31](#_Toc490210758)

[3.4.2 User Authorizations (Consent) for Data Collection and Use 32](#_Toc490210759)

[3.4.3 Pairing (Syncing) User Accounts with Devices and Data Repositories 33](#_Toc490210760)

[3.4.4 Security for Data at Rest 34](#_Toc490210761)

[3.4.5 Security for Data In Transit 35](#_Toc490210762)

[3.4.6 Data Authenticity, Provenance, and Associated Metadata 35](#_Toc490210763)

[3.4.7 Data Exchange and Interoperability 37](#_Toc490210764)

[3.4.8 Notifications and Alerts 37](#_Toc490210765)

[3.4.9 Product Upgrades 38](#_Toc490210766)

[3.4.10 Audit 38](#_Toc490210767)

[3.5 App Service Termination 40](#_Toc490210768)

[3.4.11 App and Data Removal 40](#_Toc490210769)

[3.5.1 40](#_Toc490210771)

[3.5.2 Permitted Uses of Data Post Account Closure 41](#_Toc490210772)

[3.6 Nonfunctional Requirements: Conditions and Agreements 41](#_Toc490210773)

[3.6.1 Conformance 41](#_Toc490210774)

[3.6.2 Related Regulations, Standards, and Implementation Tools 42](#_Toc490210775)

[3.6.3 Implementation Guidance 42](#_Toc490210776)

[4 Definitions 43](#_Toc490210777)

[4.1 Definitions of Alerts and Notifications 43](#_Toc490210778)

[5 Implementation 47](#_Toc490210779)

[5.1 Device- or OS-specific Considerations 47](#_Toc490210780)

[6 Appendices 48](#_Toc490210781)

[6.1 Reference Documents 48](#_Toc490210782)

[6.2 Version History/Change Log 49](#_Toc490210783)

[6.3 Relationship to Other Standards 49](#_Toc490210784)

# Introduction

## Acknowledgements

To be added

## Background

As of 2015 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 for consumers, but also for clinicians, who may consider recommending or prescribing use of an app to help track and improve health behaviors and in the ongoing monitoring of chronic health conditions.

The Framework acknowledges that 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. Within Section Two three exemplary use cases of increasing complexity are introduced and serve to guide development of the Framework.

## Intended Audience

1. cMHAFF is primarily directed at **developers of mobile health apps for consumers**, to assist them in building apps that protect consumer privacy, security, data access, etc.
2. Secondarily, cMHAFF is directed at organizations (such as test labs, certification bodies, professional societies, or “consumer reports” types of organizations) that will test, assess, or endorse mobile apps, for conformance to essential criteria.
3. cMHAFF can also be informative as a checklist for prospective purchasers of mobile apps (e.g., consumers, or providers on behalf of consumers).
4. The beneficiaries of cMHAFF will primarily be consumers, due to improvements in apps and in their consumers’ increased understanding and assurance. But those who receive information from consumers, such as providers, caregivers, and researchers, can also be beneficiaries. Some provider organizations, such as the American Medical Association, have published principles[[1]](#footnote-1) to ensure accurate, effective, safe and secure mHealth apps.

## How to Use this Guide

The questions in this section help the reader determine which conformance subsections of cMHAFF should be read by the intended audience. Each subsection of 3.x 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. In addition to these questions, all USA mobile app developers should consult the 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> cMHAFF does not duplicate the FTC questions.

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 actions depending on the answer to that question.

|  |  |
| --- | --- |
| **QUESTIONS** | **DECISIONS BASED ON ANSWERS** |
| The following sections of cMHAFF should be reviewed by any Mobile App developer, no matter how simple the app.  | 3.2.x, 3.4.8 (Product Upgrades) |
| Does the app handle patient-identifiable information? | YES – then sections 3.3.x (download and install app), 3.4.1 (authentication), 3.4.2 (authorization), 3.4.9 (audit), 3.5.1 (app and data removal), and 3.5.2 (permitted uses post closure) from cMHAFF applyNO – then those sections from cMHAFF do not apply |
| Does the app offer health records directly to consumers (or does it interact with or offer services to someone who does)? | YES – FTC Breach notification rule applies |
| Does the app store or transmit data outside the mobile device, e.g., the cloud or another HIT system? | YES – then cMHAFF 3.4.4 (security for data at rest), 3.4.5 (security in transit) and 3.4.6 (data provenance, authenticity) apply |
| Does the app connect to sensors or other types of devices that gather measurements of the patient’s condition? | YES – then cMHAFF 3.4.3 (pairing), 3.4.5 and 3.4.6 also apply |
| Does the app send alerts or notifications to the user? | YES – then cMHAFF 3.4.7 (notifications and alerts) applies |
| FTC Questions below – included here temporarily, but will not be included in the decision tree.  |  |
| Is the app developer a healthcare provider or health plan? | YES – HIPAA applies.  |
| Is this app developed on behalf of a HIPAA covered entity (such as a hospital, doctor’s office, health insurer, or health plan’s wellness program)? | YES – HIPAA Business Associate, HIPAA Security rule and parts of HIPAA Privacy and Breach Notification rules apply |
| Is the app intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease? | YES – it’s a medical device, see next question |
| Does the app pose “minimal risk” (see definition[[2]](#footnote-2)) to a user? | NO – See next question |
| Is the app a “mobile ***medical***app” (see definition[[3]](#footnote-3)) | YES – FDA regulatory oversight applies |

**Alternative Decision Tree Presentation (from unpublished EU Guidelines)**



For this current round of HL7 balloting, reviewers are asked to: 1) critique the form of the Framework; 2) make recommendations concerning changes and additions to conformance criteria; 3) extend lists of resource references, including references to other HL7 standards; 4) and respond to questions specific to each section as posed by the authors. The intent of the Mobile Health Work Group is to use this feedback to improve the quality and relevance of the Framework and create a version of the Framework to be balloted as Informative or a Standard for Trial Use (DSTU) in 2017.

Section 3 forms the core of the Framework. Each section addresses security, privacy and data concerns based on a given stage of the app lifecycle through the following format:

* ***Conformance criteria***: Criteria consist of items applicable to all consumer health apps and criteria 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. Conformance criteria within the Framework focus on issues of high importance as to create a standard which is lightweight. As such, criteria are heavily weighted toward those with a force of “SHALL” with much fewer which have forces of “SHOULD” and “MAY”.
* ***Related regulations, standards, and implementation tools***: References to documents which can help an app developer or promoter are included. Regulations and standards can provide additional realm-specific guidance, and implementation tools can help in the creation of apps which have focused relevance and which are consistent with consensus opinions of relevant styles and interaction designs.
* ***Implementation guidance***: Guidance for app developers is included. As applicable, the differential application of conformance criteria by type of app is discussed, referencing the model use cases described in Section 2.

# Overview

## Goals

The primary goals of the HL7 Consumer Mobile Health Application Functional Framework 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. Another goal is to promote the generation of health data which is reliable and actionable. 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 the Framework.

The decision to create a standard focused on a smaller set of criteria was made to make the standard both developer-friendly and easy to update on a frequent basis. However, it is important to note that the Framework is NOT creating a standard which is easy to meet. The Framework challenges market assumptions concerning the 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, the Framework can potentially provide a path to assessments that can span a range including self-attestation, testing, endorsement[[4]](#footnote-4), and/or certification (voluntary or regulatory). cMHAFF is developed independent of the method of assessment, but aims to be suitable for use for 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.

1.
2.

## Scope

### In Scope

This framework focuses specifically on **consumer** mobile apps than run on devices such as smartphones, tablets, and wearables. It is focused on the **general** capabilities, that can be thought of as “horizontal” features that are applicable to most or all apps, rather than to the specific health, clinical, or medical functionality of an app.

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 (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

* Security
* Privacy
* Permission to use device features
* Data Access
* Data Sharing
* Information for consumers (e.g., App Store descriptions, product disclosures)
* Terms of Use, Conditions
* Product Development, including user-centered design and compliance with applicable regulations
1.
2. 1. 1.

### 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 not consumer-focused.
* Clinical or health app functionality (e.g., diabetes monitoring, exercise calculations). The Mobile Health workgroup does not have the subject matter expertise to define those types of criteria.
* 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 (e.g., cMHAFF is not directed to Apple, Google, Samsung…).
* 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.
* 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 sections 3.x follow a lifecycle model in relation to a consumer’s use of a mobile health application, from first finding an app in an App Store to disuse and de-installation.

**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, conformance statements in Section 3 of 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 which may be applied to any app. Use Case C is the most sophisticated and generates the most requirements. Its description includes examples of the risk factors that should be considered by developers and users.

Section 3 (Conformance Criteria) includes discussion of considerations as to how subsets of conformance criteria can be addressed in different manners, referencing the use cases in this section as a way to provide directional, rather than pinpoint, guidance.

### Use Case A: Simple, Standalone

A walking app collects data based on how far someone walks, using GPS technology. A consumer can view a history of walks taken and summary statistics related to distance walked and estimated calories burned. App developer is not a HIPAA-covered[[5]](#footnote-5) entity (CE), nor is the app sponsored by a CE (such as a hospital or physician).

 

|  |  |
| --- | --- |
|  | Simple |
| FDA App Categorization | Wellness |
| FDA Data Device Categorization | None |
| PHI Data Storage | Smartphone |
| Data transmission by App | None |
| Importance of Data Integrity | Low |
| HIPAA covered? | No |

### Use Case B: Device-Connected Wellness App

A weight management app helps 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 a 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): these make it potentially a medical device and candidate for government regulation, though not at this time.[[6]](#footnote-6) The app has an ability to download weight, activity, and food consumption information to PHRs through a published API. In the US Realm, the App developer is not a HIPAA entity, but app can be white-labeled by HIPAA entities, such as a clinic offering a PHR to its patients through a portal.

 

|  |  |
| --- | --- |
|  | Device Integrated |
| FDA App Categorization | wellness |
| FDA Data Device Categorization | regulated device |
| PHI Data Storage | smartphone/PHR |
| Data transmission by App | device-app-PHR |
| Importance of Data Integrity | mid |
| HIPAA covered? | no, but yes, if white-labeled |

### Use Case C: EHR-Integrated[[7]](#footnote-7) Disease Management App

A diabetes management app allows a consumer to collect blood sugar readings through a Bluetooth-enabled glucometer. The app is offered by the provider, a HIPAA covered entity. Its purpose is to allow the patient’s blood sugar to be captured through devices, rather than relying on manual entry by the patient, and to electronically transmit the readings to the patient’s physician, rather than relying on paper or FAX logs. Activity information is collected through an activity tracker, and a consumer can open the app and tap icons when they have a meal or a snack to enable estimates of caloric consumption. Collected data is automatically “pushed” to a third-party cloud-based platform. The patient is aware of the cloud platform, though not familiar in detail with how data are protected in transit or as stored. When a consumer views information on their smartphone which shows daily glucometer readings and related information, this information is “pulled” into the app but does not persist on the smartphone when the app is closed. It is also possible for the consumer to directly enter blood sugar readings (e.g., using backup manual glucometer if Bluetooth device is not working). From the cloud platform, consumer information is “pushed” to a provider’s Electronic Health Record (EHR) of the patient[[8]](#footnote-8), where it is accepted as Patient Generated Health Data (PGHD), according to the preferences of the patient and the policies of the provider. From the EHR, a physician can set upper and lower boundaries for blood sugar readings such that the consumer is alerted through the app when a measurement is out of range. From the EHR a physician can create logic which sends an alert to the consumer’s care manager when a set number of high or low readings are noted within a prescribed period of time.

 

|  |  |
| --- | --- |
|  | EHR Integrated |
| FDA App Categorization | medical |
| FDA Data Device Categorization | FDA regulated device |
| PHI Data Storage | cloud/EHR |
| Data transmission by App | device-app-cloud-EHR |
| Importance of Data Integrity | high |
| 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.

|  |  |
| --- | --- |
|  |  |

The following are additional risk scenarios that may be considered for cMHAFF conformance criteria to mitigate them. (🡺Suggested mitigations are listed in parentheses)

* Consumer loses their device. Confidential information is handled by the app, and there is risk of information disclosure (🡺 3.4 encryption of data, automatic timeout/logoff)
* The device can be lost or damaged, impeding the consumer’s use of the app, thereby impacting their care, even if privacy is protected. (🡺 backup of data, ability to restore to new device)
* Someone else uses consumer’s device either by permission or unintentionally (🡺 automatic timeout/logoff)
* 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 a feature if app handles PHI)
* The app is used and left open, where others could see it while the device is unlocked (🡺 automatic timeout/logoff)
* Measurements are not captured accurately or not transmitted accurately, and consumer takes action based on inaccurate measurements (🡺 quality management, disclosure of evidence)
* A data collection device paired with the mobile phone may in fact be for a different person (mis-association of data) (🡺 3.3, Pairing User Accounts. #2)
* A third party cloud-based platform may have inadequate security measures of which the consumer is unaware. (🡺 automatic timeout/logoff)
* Transmission between mobile app and cloud-based platform may have inadequate or unknown transmission security (🡺 3.5 encryption of data in transit)
* 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. (🡺 see 4.1 App and Data Removal, 4.2 Permitted Uses of Data Post Account Closure)
* The device is not on the person, is turned off, is silent, or is otherwise unable to get the consumer’s attention when the app issues an important alert. (🡺 is there a suitable mitigation?)
* 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)

Some of these potential risks are motivators for many of the conformance criteria in cMHAFF. Where risks have both high likelihood and high impact, SHALL criteria are indicated.

### Summary of Major Differences in Use Case Scenarios

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

## Environmental Scan

Summarize key points from environmental scans, including FHIRFrame survey, Gora’s State of Mobile, and other literature such as FTC Guidelines for Mobile Apps, FTC guidance on disclosures, ONC NCE report, FDA SW as medical device new guidance

* ONC/Accenture Patient-Generated Health Data white paper (draft) <http://pages.himss.org/b0001RLG5Z40WbJK030PA6V>,
* 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/>

# Conformance Criteria, Resources, and Implementation Guidance

## General Considerations

Each section follows a common format. Criteria are separated from “force”. That is, each criterion stated in a neutral way, and the optionality of addressing the 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 in Internet 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 be understood 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 or because 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 include the option (except, of course, for the feature the option provides.)

[IF] The stated force applies when the clause in brackets is applicable to the product. When the clause does not apply, no conformance is expected.

1.
2.
3.

## Product[[9]](#footnote-9) Development and Support

Prior to marketing a mobile app, the developer has a responsibility to ensure it meets Realm-specific rules and regulations. The security and privacy of information used by the app needs to be considered throughout the development of the app: planning, coding, and testing. Assessing the usability of the app helps ensure the app’s viability and adoption; testing must be population-relevant and demonstrate reasonable product usability by people with visual, auditory and motor disabilities. Establishing a system of customer support enables product defects and usability issues to be surfaced in a systematic way and helps users to effectively resolve problems related to use of the app.

* 1.
	2.
1.
2. 1.
	2.

### Regulatory Considerations

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
|  | SHALL | Following Realm-specific regulatory rules, determine if the app needs regulatory approval before the app is used by the general public. For example, in the US realm this would include 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. | App Owner or Developer |
|  | SHALL[IF] | [App requires regulatory approval] Regulatory approval is obtained before app is made available to the general public. | App Owner or Developer |
|  |  |  |  |

#### Related Regulations, Standards, and Implementation Tools

* Federal Trade Commission **Mobile Health Apps Interactive Tool** (to help USA developers know which federal laws apply)
<https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool>
* EU Privacy Code of Conduct on Mobile Health Apps. <https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps>
* EU 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>
* Office of Civil Rights (OCR): **Health App Use Scenarios & HIPAA**, Guidance to USA Health App developers regarding HIPAA applicability
<http://hipaaqsportal.hhs.gov/>)
* U.S. Food and Drug Administration: Web page of guidance on Mobile Medical Applications, <http://www.fda.gov/medicaldevices/digitalhealth/mobilemedicalapplications/default.htm>
and more specific guidance on medical devices, published February 9, 2015
* <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf>

#### Implementation Guidance

* Use Case A: In the US Realm, a walking app which encourages general wellness is not considered a medical device 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 medical device 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.

### Product Risk Assessment and Mitigation

This section deals with process steps for those who are developing an app, prior to its being deployed to consumers. If some information identified during this step should be disclosed to consumers, that is stated in the “Informing Consumers/Users” section.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | Complete a product risk assessment using an established risk management framework. The framework should provide ample assessments to effectively determine risk of inappropriate disclosure of medical information. | App Owner or Developer |
| 2 | SHALL[IF] | Rank 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). | App Owner or Developer |
| 3 | SHALL | Create and document a product risk mitigation plan. 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. | App Owner or Developer |
| 4 | SHALL | In development, follow secure coding practices using an established framework. | App Developer |
| 5 | SHALL | In development, test for security flaws in the app using defined scripts which can be executed using automated methods and/or by human testers. | App Developer |
| 6 | SHOULD | Prior to product launch, complete User Acceptance Testing (UAT) by testers who are not part of the formal development team. Often this will include product business owners. | App Owner or Developer |
|  |  |  |  |
| 7 | SHOULD | Monitor and document conflicts or compatibility issues of the app with other apps, device features (e.g., camera), or connected devices. | App Owner or Developer |
| 8 | SHALL[IF] | [app is intended for use by professionals or transmits data to an EHR] Document failure rates, measurement error rates, software bugs, and hardware risks of all types. | App Owner or Developer |
| 9 | SHOULD[IF] | [app relies on external supporting infrastructure, (e.g., cloud-based servers) to operate] Document measures to ensure the availability of that infrastructure | App Owner or Developer |
| 10 | SHOULD | Have measures to safeguard minors in accordance with applicable regulations.  | App Owner or Developer |

#### Related Regulations, Standards, and Implementation Tools

* **ADD FRENCH H.A.S. GOOD PRACTICE GUIDELINES, Andalusian Guidelines…**
* 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 app developers, so most of it is pertinent to cMHAFF.
* (DRAFT) NISTIR 8144 Assessing Threats to Mobile Devices & Infrastructure, *The Mobile Threat Catalogue*
<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 of the threat catalog closest to cMHAFF)

#### Implementation Guidance

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 consumer’s target environment, rather than the developer’s own environment. Because of the diversity of consumers, such a risk analysis is wider ranging and more challenging than a risk analysis for a single organization’s controlled environment.

### Product Usability

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | Assess product against an industry-validated usability assessment tool, using subjects who are demographically-similar to intended users (target audience). |  |
| 2 | SHALL [IF] | [intended users include those with motor disabilities] Assess product for usability by people with motor disabilities.  |  |
| 3 | SHALL [IF] | [intended users include those with visual disabilities] Assess product for usability by visually-impaired people using a standard mobile screen reader. |  |
| 4 | SHALL [IF] | [intended users include those with auditory disabilities] Assess product for usability by people with auditory disabilities. |  |
| 5 | SHOULD | Assess product for usability by a sample of intended users. If geared towards a certain age segment or to people with a specific chronic health condition, usability testing subjects are drawn from these populations. |  |
| 6 | SHOULD | Create a written usability assessment plan, including known problems with product usability and mitigation plan. NOTE: for U.S. Realm when an app is sponsored by a HIPAA entity, the force of this criteria is elevated to “Shall” with plan specifically addressing usability issues for people with visual and motor disabilities. |  |
| 7 | SHOULD | Follow design/style guide standards established by the platform provider(s) for the app, e.g., Android, iOS, Windows… |  |
| 8 | SHOULD | Avoid excessive data use by the app, minimizing it as much as possible warning users when high data usage occurs (e.g., downloads and updates). |  |
| 9 | SHOULD | Describe the use cases (business scenarios) and intended users for the App’s main functions |  |
| 10 | SHOULD | Permit flexibility (adaptation) to the user’s specific abilities, needs, or requirements |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

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.

### CUSTOMER/TECHNICAL SUPPORT

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | Information as to how to access customer support, and channels of support (e.g., voice, email, text, Twitter, etc.) is clearly stated within the app’s Terms of Use and as a feature accessible from within the app. |  |
| 2 | SHALL | Customer support may be accessed 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). |  |
| 3 | SHALL | Customer support queries will 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. |  |
| 4 | SHALL | Customer support is provided in the language(s) in which the app is published. |  |
| 5 | SHALL | 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 is given attribution. |  |
| 6 | SHALL[IF] | [Support request involves accessing, disclosing, or changing customer data] The identity of the customer, and the customer’s data access rights, must be verified before any disclosure or changing of customer data. |  |
| 7 | SHOULD | Provide app consumers with aggregated satisfaction ratings relevant to customer support terms and conditions as appropriate. |  |
| 8 | MAY | A comprehensive performance dashboard is publicly available and offer features for comparison with similar or competing apps |  |
| 9 | SHOULD | Provide a FAQ resource where users can find answers to common questions. |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

## Download and Install App

Apps are most 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. These conformance criteria intend to harmonize certain characteristics of app descriptions and access to information about intended uses of data and privacy controls.

### Informing Consumers/Users

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.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  | **GENERAL INFORMATION** |  |
| G1 | SHALL | The description of an app includes the main functionality and intended use of the user’s personal data by the app. |  |
| G2 | SHOULD | The app description should clearly state the intended (target) audience, including the human languages the app supports.  |  |
|  |  |  |  |
|  |  |  |  |
| G3 | SHALL | Screen shots of the app accurately depict the screens of the product. |  |
|  |
|  |  |  |
| G4 | SHOULD | State that the use of the app does not replace the provider-patient relationship or the recommendation, opinion, or diagnosis of a health professional. |  |
| G5 | SHOULD[IF] | [App is of criticality level \_\_\_\_] Advise customers to approve health app selections with their personal medical team.  |  |
| G6 | SHOULD | Provide information about accessibility characteristics in the app description and in contextual assistance sections of the app. |  |
| G7 | SHOULD | Provide information about the app owners (persons/organizations) and provide mechanisms to communicate with the owners | Publisher |
| G8 | SHOULD | Provide disclosure 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 owner. | Publisher |
|  |  | **PAYMENT** |  |
| P1 | SHALL | The payment amount for the app, if any, must be clearly noted according to app store rules. |  |
| P2 | SHALL | Apps which have required or optional payments after download must 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). |  |
|  |  | **EVIDENCE/CREDENTIALS** |  |
|  |  |  |  |
| E1 | SHOULD | The app descriptions should identify the health professionals and credentials of those who worked on the app and/or at least the medical organization that made, reviewed, or sponsored the app.  |  |
| E2 | SHALL[IF] | [App is of criticality level XXXX] Disclose the scientific degree of evidence and the types of sources used (e.g., clinical practice guidelines and protocols, peer-reviewed articles, professionals and organizations with their credentials) that guided the app content. |  |
| E3 | SHOULD[IF] | [there is human and/or automated interpretation of health-related content] The credentials of qualified health professionals are disclosed, and/or the algorithms and testing plans and reports are documented. |  |
| E4 | SHOULD | Show the date of the last update to the app, and describe the changes from the previous release (e.g., revisions due to new scientific evidence). |  |
| E5 | MAY | The app description may also include data related to app reliability and validity tests or population research results. |  |
|  |  |  |  |
| E6 | SHOULD | Declare the degree of admission of liability regarding the selection and use of the content. | Publisher |
|  |  | **LIMITATIONS AND WARNINGS** |  |
| L1 | SHOULD | Document contraindications, potential risks and limitations of use in documentation available for consumers to consult. For example, environmental or patient conditions under which apps or connected devices may be unreliable, e.g., tattoos that impact optical sensors). |  |
| L2 | SHOULD | Warn users of updates caused by possible errors in functioning, in health-related information, or in any other sensitive data. |  |
| L3 | SHALL[IF] | [App is of criticality level XXXX] Disclose the potential risks to patient safety. |  |
|  |  | **TECHNICAL DETAILS** |  |
| T1 | SHALL[IF] | [user can enter personal health information into the app] Clearly disclose whether or not data validity checking is done, and document or reference the evidence for such validity checking |  |
| T2 | SHALL[IF] | [App collects or receives quantitative data] The precision (accuracy) of measurements (e.g., physical activity, physiological data from connected devices) is documented and appropriate for the intended use of the App.  |  |
| T3 | SHOULD[IF] | [App collects or receives quantitative data] The smallest level of data measured (granularity) is documented and justified by the intended use of the App.  |  |

#### Related Regulations, Standards, and Implementation Tools

* French GPG
* Andalusian Guidelines
* Federal Trade Commission Disclosure Guidelines?

#### Implementation Guidance

### Launch App and Establish User Account

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | A user can review the app’s Terms of Use before personal data about the user is collected or used. |  |
| 2 | SHALL [IF] | [the app creates user accounts] User acceptance of the app’s Terms of Use is logged before a user account is authorized. (See Section 3.11 for information about audit log record creation.) |  |
| 3 | SHALL | For purposes of establishing an account, the minimum amount of a user’s personally identifiable information (PII) is collected. |  |
| 4 | MAY | For children, require verification of age or documented approval from parent or guardian where required by law. |  |
| 5 | SHALL [IF] | [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,1. The user is informed about what attribute information will be used by the app associated with the pre-existing credentials;

The user is informed about what data is communicated back to the IDP at the time of account creation and at each subsequent user authentication. |  |
| 6 | SHALL[IF] | [Access to account exposes Protected Health Information (PHI) or PII] The user is given an option to utilize strong authentication methods (e.g., multi-factor authentication and/or biometrics) in addition to passwords, in subsequent authentication attempts to the app. Before selection of this option, the mechanism for authentication is clearly described and/or demonstrated to the user. |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

* 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

## Use App

### User Authentication and Authorization to Access App Services

Introductory text to be added.

#### Conformance

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.

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | The identity of an app user is authenticated prior to any access of PHI or PII. The method of authentication is communicated to the app user when an app account is established.  |  |
|  | SHALL [IF]? | [EHR is a system actor] IDENTITY PROOFING CRITERIA TO BE ADDED. Need to ensure that the remote access is legitimately from the real account holder. At app registration time, the API Provider may need assurance of the identity of the app developer; at app approval time the API provider needs assurance of the consumer’s identity and the patient may need assurance of the app’s authenticity; at data access time, the API provider may need assurance of the app’s authenticity in order to permit access.  |  |
| 2 | SHALL | The app user is 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. |  |
| 3 | SHALL [IF] | [EHR is a system actor][[10]](#footnote-10) The EHR authorizes an app user’s access to app features when these features are supported by data provided by or written to the EHR. |  |
| 4 | SHALL | At the request of an app user, the app terminates such that access to PHI or PII requires a new, successful authentication attempt. |  |
| 5 | SHALL | The app terminates access to PHI or PII after a period of time of disuse as described in the app’s Terms of Use. This feature is sometimes called “automatic 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 though the app.  |  |
| 6 | SHALL[IF] | [passwords are stored on the device] passwords are encrypted.  |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

See Section 2.2 for a discussion as to the selection and ongoing use of a user authentication mechanism.

* NIST: Measuring Strength of Identity Proofing, December 16, 2015, https://www.nist.gov/sites/default/files/nstic-strength-identity-proofing-discussion-draft.pdf
* API Task Force Final Report, May 12, 2016: https://www.healthit.gov/facas/sites/faca/files/HITJC\_APITF\_Recommendations.pdf Specifically, Topic 8 recommends that identity prooffing for apps be the same as for MU2-era patient portal sign-in and View/Download/Transmit.

### User Authorizations (Consent) for Data Collection and Use

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | Smartphone functionality and data sources may only be used when it is essential to the functioning of the app. This includes the use of: location services, camera, microphone, accelerometer, contact lists, calendars. |  |
| 2 | SHALL | Before using select smartphone functions and data sources for the first time, app users are asked for permission to use these services and data sources. Permissions for each function, data source and user tracking activity controlled by the app are asked as individual questions while the app user is interacting with the app. This includes the use of: location services, camera, microphone, contact lists, activity tracking, calendars, and other available sensors. |  |
| 3 | SHALL | Before exporting data from the smartphone, or from any device integrated with the smartphone, the app user is 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.  |  |
| 4 | SHOULD | An app user can choose to permit some, but not all, requested data to be exported from a smartphone or associated device. The user is informed as to how the choice to limit data effects the functionality of the app. |  |
| 5 | SHOULD | [app user denies a permission requested by the app] The app user is informed of the consequence of not extending the permission and is given a second chance to extend a permission. |  |
| 6 | SHALL [IF] | [app requests permission to use data generated by the app after it is de-identified] Account holder is informed of who would have access to the de-identified data and for what purpose. |  |
| 7 | SHALL [IF] | [app requests permission to use data generated by the app after it is de-identified] Account holder is informed of the possibility that de-identified data can potentially be re-identified and steps the app sponsor takes to prevent re-identification. |  |
| 8 | SHALL [IF] | [user gives permission for data generated by the app to be de-identified and used] Data de-identification, at minimum, follows HIPAA safe-harbor rules. |  |
| 9 | SHALL [IF] | [in-app payments exist]. In-app payments are not triggered in such a way that can expose healthcare-related information to payment organizations. |  |
| 10 | SHALL [IF] | [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.  |  |
| 11 | MAY | Share data with social networks, only after obtaining explicit user consent |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

### Pairing (Syncing) User Accounts with Devices and Data Repositories

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | User has authenticated identity to an app and has an active session before pairing an external device to an app account. |  |
| 2 | SHALL | Before a device is paired with an app to collect information about a specific individual, the app displays 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. |  |
| 3 | SHALL | The person who pairs a device with an individual in context of use of a specific app can un-pair the device and individual through an app utility. |  |
| 4 | SHALL | Before a device is paired with an app to collect information about a specific individual, the app states 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. |  |
| 5 | SHALL [IF] | [Data for more than one person can be collected by the app/device pair] The app asks the account holder to confirm the person for whom data will be collected by the device before data is collected and transmitted. |  |
| 6 | MAY | Offer an option to sync data across multiple devices, with user’s consent (e.g., same app data synchronized across smartphone and tablet devices) |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

### Security for Data at Rest

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | PHI and PII stored on a smartphone is stored as encrypted values. |  |
| 2 | SHALL | PHI and PII stored by the mobile app on any external server is stored as encrypted values  |  |
| 3 | SHALL | 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. |  |

#### Related Regulations, Standards, and Implementation Tools

Comment

#### Implementation Guidance

Encryption paradigms should follow contemporary practices as the strength of an encryption method may degrade over time as computational methods for breaking encryption continue to evolve.

### Security for Data In Transit

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | PHI and PII transmitted between an app and an external data source, including data generated through a device associated with the app, are transmitted as encrypted values. |  |
|  |  |  |  |

#### Related Regulations, Standards, and Implementation Tools

Comment

#### Implementation Guidance

### Data Authenticity, Provenance, and Associated Metadata

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | Apps conform to Best Practices for Data Authenticity, Provenance, and Associated Metadata  |  |
| 2 | SHALL[IF} | [App itself originates data <see draft ISO 21089 definition of originate>] Customer has review option which includes the option to irreversibly destroy, reject or discard data. |  |
| 3 | SHALL[IF} | [App itself only receives data as a “pass through” and cannot store data] Customer has a review option to display the data prior to executing the pass-through which includes the option to irreversibly stop and block the pass-through. |  |
| 4 | SHOULD[IF] | [App itself receives data and stores it] Customer has 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 have the option to delete the original data.  |  |

#### Related Regulations, Standards, and Implementation Tools

Cornell University has federal rules of evidence [need specific reference]

Should there be reference to HL7 DPROV or FHIR Provenance?

#### Implementation Guidance

As permitted by the Account Holder and supported by the app, someone other than the Account Holder is able to access the system

[App generates data to a persistent record for ongoing clinical decision making]

Capturing different specifications for what constitutes data authenticity and provenance and necessary supportive metadata. Some Realms have definite concepts on what constitutes reliability. At the minimum, specifications should support US Realm Business Records requirements according to the Federal Rules of Evidence. [can be distilled to 15-20 lines of prose].

Digital signature standards exist—seems like digital sigs. Human validation could sub

Record reviews “tripped” when there is NOT external validation.

If information from an app is not otherwise validated by a trusted agency, a trust protocol must be part of the device validation. [add sources].

Persistent records + NOT from a device with validation, THEN . . .

Reviewer#1: We would best revisit the topic of what to call the class of activities we're outlining for supporting data quality, etc., I think validation may actually stand up. Attestation being one type of validation.

Verify assumes specifications to verify against. Verify has no or limited meeting without knowing the verification criteria and what the object is verified against. Could be sufficient to say one or more specification types may apply. “verification” includes a number of concepts. In paper world, was impossible to segregate in any meaningful way, terms such as “verify” “attest” “certify” are used in a free form way. Is this idea not yet ready, but may have arrived in the circumstance of a relatively small subcategory of consumer mobile apps where info is intended for end use with specifications (e.g., clinical decision support), research design parameters are specified. E.g. in MU1, clinicians required to ATTEST to facts, but not to VERIFY (i.e., good faith effort vs true facts).Still, some went ahead and verified information accuracy. \*\*\*all data is not “equal” in terms of its value and need for precision\*\*\*

Reviewer#2: Verify and validate are concepts we currently work with. What is the action verb to determine data was not accurate.

Reviewer#1: not deeply researched this, but people working on these issue say that “verification” could reasonably considered a more specific term under “validation”. Some validation schema attempt to capture truthfulness, accuracy and then ask for proof in a referenced way.

Another term in lifecycle events is “attest”. Attestation does not imply that any rigorous evaluation has occurred. There is a fuzzy notion that I attest based on who I am, not the quality of the data (qualified to make a good-faith statement). “to the best of my knowledge”

Reviewer#2: testing/validating data—look to VW and recent issues.

Reviewer#3: this aligns with chain-of-evidence. Mistakes amplify.

Reviewer#1: one of the problems is that in the current marketplace, can’t say who does this well and who does not.

### Data Exchange and Interoperability

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHOULD[IF] | [App exchanges discrete clinical data] Use standard terminologies (e.g., SNOMED CT, LOINC…) |  |
| 2 | SHOULD[IF] | [App exchanges discrete clinical data] Use standard exchange for format/content, e.g., HL7 FHIR or HL7 Consolidated CDA. |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

### Notifications and Alerts

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL  | Opt-in consent is required by the account holder before receiving notifications and alerts from an app. |  |
| 2 | SHALL | To consent to receiving a notification or alert from an app, the account holder is informed of both the content and channel (SMS, push notification, email, etc.) of the notification or alert. |  |
| 3 | SHALL | An account holder can change consent decisions about notifications and alerts through settings available on the device on which the app was downloaded. |  |
| 4 | SHALL | As permitted by the account holder, notifications and alerts may be sent to the account holder or to another person or entity. |  |
| 5 | SHALL | Notifications and alerts contain the least amount of information necessary for the recipient of the alert to take a focused action. |  |
| 6 | SHALL [IF] | [app alerts notify user of conditions such as “abnormal” or “exceptional” or “out of range”] Document or reference the sources (evidence base) of the formulas/algorithms upon which such alerts and notifications are based.  |  |
| 7 | SHOULD | Provide alerts to notify the user of potential faults that could cause inconvenience or harm to the user, e.g., lower battery alerts.  |  |
| 8 | SHOULD | Notify the user in case of external interruptions or delays (e.g., loss of network connection, database problem, lengthy operation) |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

### Product Upgrades

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | The app respects operating system level permissions concerning automatic product updates. |  |
| 2 | SHALL [IF] | [an updated version of the app includes updated terms of use] Updated Terms of Use are presented 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. |  |
| 3 | SHALL [IF] | [automatic app updates are not enabled] The app prompts the user to the availability of a new version of the app when a new version is available.  |  |
| 4 | SHALL [IF] | [account holder elects to not install a new version of an app] The consequences of not installing the new version of the app, including information about support limitations for the older version of the app, are presented to the account holder. |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

### Audit

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL[IF] | [User authentication is required to access app] User authentication attempts, both successful and unsuccessful, generate an audit record. |  |
| 2 | SHALL | 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) generate an audit record. |  |
| 3 | SHALL[IF] | [App uses external devices or data sources for data collection] Pairing a device or data repository external to the app, which supplies data used by the app, generates an audit record. |  |
| 4 | SHALL[IF] | [App allows for the export of data to a data repository external to the app] Any export of data from the app generates an audit record. |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

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.

## App Service Termination

Health apps may be used indefinitely or for a finite period of time. 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.

### App and Data Removal

Introductory text to be added.

* 1. 1.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | An app Account Holder can remove an app from a smartphone at any time. |  |
| 2 | SHALL | An app Account Holder is informed 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. |  |
| 3 | SHALL | An app Account Holder can close an associated account or data store associated with the app. |  |
| 4 | SHALL | An app Account Holder is informed of the consequences of deleting the account and is given an opportunity to confirm closing the account before it is closed. |  |
| 5 | SHALL | After deleting an account associated with an app, the Account Holder is informed of what data associated with the account persists, and the Account Holder’s rights in terms of access and deletion of that data. The user should be informed 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. Deleting the account will not delete the data that is now in the EHR. |  |
| 6 | SHOULD | Before closing an app account, the account holder can 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). |  |
| 7 | SHALL [IF] | [the device permits remote or external access to device data] Any PHI or PII stored on a device can be wiped remotely by the account holder without deleting the account which is related to the wiped data. |  |
| 8 | SHOULD | Clear criteria are 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 period.  |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

### Permitted Uses of Data Post Account Closure

Introductory text to be added.

#### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 | SHALL | Data associated with an app account is not released to any new persons or entities. This includes data which has been de-identified. |  |

#### Related Regulations, Standards, and Implementation Tools

#### Implementation Guidance

## Nonfunctional Requirements: Conditions and Agreements

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. 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 must 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.

### Conformance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Strength | Requirement | Suggested Actor |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 | SHALL [IF] | [rewards are given for app participation] 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.  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 4 | SHOULD | The consumer should indicate that they acknowledge and understand the app functionality |  |
| 5 | SHALL [IF] | [app includes in-app payments] The app description shall disclose what is included as base functionality without payment, and what functionality would require additional payment. |  |
| 6 | SHALL [IF] | [App permits in-app payments] The benefits for paying for a service or feature are clearly stated in a manner which allows an account holder to make an informed decision about making or declining an in-app payment. |  |
| 7 | SHALL [IF] | [App access is by subscription] The requirements for cancelling a subscription are clearly stated in the CnA.  |  |
| 8 | SHALL [IF] | [App requires an additional charge to upgrade] The upgrade charges, the amount of advance warning for upgrades, and the length of support for the old version (if not upgraded) are clearly stated in the CnA.  |  |
| 9 | SHOULD | Disclose the use of advertising mechanisms, distinguish advertisements from app content, and provide ways to deactivate or skip advertisements.  |  |

### Related Regulations, Standards, and Implementation Tools

* 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*](https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf)
* French H.A.S. Good Practice Guidelines

### Implementation Guidance

# Definitions

## Definitions of Alerts and Notifications

The following text was written in March 2016 as a standalone document for cMHAFF discussions. It has been copied here, unedited at first, but it will be edited to make it appropriate for this document. .

Philosophically, the MH group 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 should take note of that, and acknowledge the various uses.

Even limiting ourselves to the consumer mobile space, there are multiple platforms – predominantly Apple (iOS), and Google (Android). Microsoft Windows market share is much smaller. Each has different terms that are used in apps for their mobile devices. For an HL7 standard, we should seek terms that are generic and platform-neutral wherever possible, and map these generic terms to platform-specific terms. 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 don’t 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.

The following table proposed suggested standardized (generic) terms in the left column, with mappings to three platforms in the middle three 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, Microsoft).

Despite the proposed granularity of these terms, that does not mean that there need to be separate cMHAFF 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 of notifications.

| Suggested “standardized” (generic) term for cMHAFF | Apple (iOS) equivalent | Google (Android OS) equivalent | Windows Phone | Comments**[[11]](#footnote-11)** |
| --- | --- | --- | --- | --- |
| MessageAny 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[[12]](#footnote-12) 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. | Sometimes used to describe the purpose or content of one of the notification types, e.g., a toast can be described as a short text-based message that appears to let the user know about transient data.  | 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).  |
| NotificationA device-specific message communicated to a user to inform 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.  | Notification – generic term to cover many types of notifications.  | Notification – generic term to cover many types of notifications. | Notification. Push notification is the preferred method, where notifications are pushed from a Microsoft cloud-based server to the device’s apps, rather than having each app check for its own notifications using its own method. However, alarms and reminders cannot be push notifications.  | Generic term that has subtypes. While HIT also has “notifications” that may delivered to an app, not just to a human user, let’s stick with the common consumer-based definition |
| AlertA 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 | Alarms and reminders, also collectively called “Scheduled Notifications.” These can only be done through local notifications, not push.  | 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 NotificationA 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 NotificationStatus Notifications can appear outside the app window and can be used to attract the user back to the app.  | Tile Notification, raw notificationIncrements a counter on a live tile (conceptually similar to an icon) | Android has more than one type of notification. While HIT also has “notifications” that may delivered to an app, not just to a human user, let’s stick with the common consumer-based definition |
| Temporary NotificationA 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. Do they vanish like regular banners that aren’t on the lock screen? I don’t think so.  | ToastToasts appear within the app window, not outside of it | Toast notificationAppears at top of screen for 10 seconds. When tapped, can take the user to a specific screen within the app.  | 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 NotificationA 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 of this set of definitions. Probably need a better term for this.
	+ **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)

# Implementation

## Device- or OS-specific Considerations

For Apple, Google, and Microsoft.

* <https://support.apple.com/en-us/HT201925> This article is rather loose about its terms, since it is entitled “Use Notifications” and then uses “alerts” synonymously. They speak of “banner alerts” for example, but also just “Alerts” as something where you need to act before you can move on. While this is an official Apple source, I will give preference to the following, which is Apple’s documentation oriented toward app developers, who are the primary audience of cMHAFF.
* <https://developer.apple.com/library/ios/documentation/UserExperience/Conceptual/MobileHIG/NotificationCenter.html> -- This Apple guidance uses “Notifications” as a general term, encompassing two delivery mechanisms: **local** notifications (delivered on same device as app) and **remote (“push”)** notifications sent to all devices that have the app installed. They also then talk about supporting “as many as possible of the following notification types.”
	1. Banner – translucent, disappears after a few seconds, offers users the ability to tap the banner to switch to the sending app
	2. Alert – requires user interaction to dismiss
	3. Badge – small red oval that displays the number of pending notification items for an app
	4. Sound – something that can accompany any of the above three types.

Even though Apple also speaks of local and remote as “types” of notifications, we can think of that as a distinction along a “delivery location” axis, whereas banner/alert/badge/sound are along a “user experience or style” axis.

* <http://code.tutsplus.com/tutorials/android-sdk-using-alerts-toasts-and-notifications--mobile-1949>
* <https://blog.udemy.com/android-notification-examples/>
* <https://msdn.microsoft.com/en-us/library/hh221549.aspx> -- While this page is under a thread about “game code,” I think its descriptions of Windows phone types of push notifications must be applicable to non-game apps too. It describes Toasts (similar to Android Toasts), Tiles (similar to iOS Badges), and Raw notifications. Raw Notifications are only available inside an app, when the app is running, and are not processed by the underlying OS. Since I could not find an equivalent in other platforms, I did not include this as a separate category.
* [https://msdn.microsoft.com/en-us/library/windows/apps/jj662933(v=vs.105).aspx](https://msdn.microsoft.com/en-us/library/windows/apps/jj662933%28v%3Dvs.105%29.aspx). In addition to toasts and tiles, this talks about Alarms and Reminders (like Alerts, with dialog box). Alarms and reminders display a dialog box that the user can dismiss or postpone. Unlike Tiles and toasts, alarms and reminders can only be updated with local, scheduled notifications, and not with push notifications.
* [https://msdn.microsoft.com/en-us/library/windows/apps/hh202946(v=vs.105).aspx](https://msdn.microsoft.com/en-us/library/windows/apps/hh202946%28v%3Dvs.105%29.aspx) More details on Alarms and Reminders (like Alerts).

# Appendices

## Reference Documents

* **References for Risk Assessment**
	+ HITRUST Alliance *Risk Analysis Guide* <https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf>**.** This is targeted to for health care organizations, but describes a framework that could also benefit developers of mobile health apps.
	+ National Institute for Standards and Technology (NIST), Special Publication 800-163, Vetting the Security of Mobile Applications, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf>
	This is intended to help organizations “vet” mobile apps that they acquire, but is also intended to help app developers understand potential software vulnerabilities.
* References for Usability
	+ U.S. Department of Health and Human Services, usability.gov, <http://guidelines.usability.gov/>
	+ W3C Mobile Usability, <http://www.w3.org/WAI/mobile/>
	+ Americans with Disabilities Act, Website Accessibility Under Title II of the ADA <https://www.ada.gov/pcatoolkit/chap5toolkit.htm>
	+ Web Content Accessibility Guidelines (WCAG) 2.0, <https://www.w3.org/TR/WCAG20/>
	+ User Agent Accessibility Guidelines (UAAG) Overview, <https://www.w3.org/WAI/intro/uaag.php>
	+ Mobile Accessibility is covered in existing W3C WAI accessibility standards/guidelines…there are not separate guidelines for mobile accessibility. <https://www.w3.org/WAI/mobile/>
* References for Launch App and Establish User Account
	+ US Department of Health and Human Services (HHS) Summary of the HIPAA Privacy Rule, <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.
	+ NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 2010), <https://doi.org/10.6028/NIST.SP.800-122>, for the US realm.
	+ 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.
* **References for User Authentication and Authorization**
	+ National Institute for Standards and Technology (NIST), Cybersecurity Framework, <http://www.nist.gov/cyberframework/>
* References for Authorization for Data Collection and Use
	+ ONC Model Privacy Notice (updated December, 2016) [*https://www.healthit.gov/sites/default/files/2016\_model\_privacy\_notice.pdf*](https://www.healthit.gov/sites/default/files/2016_model_privacy_notice.pdf)
	+ EU Draft Code of Conduct on privacy for mobile health applications.
	<https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps>
	+ Cross-Device Tracking Considerations [*https://www.ftc.gov/system/files/documents/public\_events/630761/cross-device\_tracking\_workshop\_deck.pptx*](https://www.ftc.gov/system/files/documents/public_events/630761/cross-device_tracking_workshop_deck.pptx)

## Version History/Change Log

## Relationship to Other Standards

* Mention HL7 EHR System Functional Model and PHR System Functional Model and their profiles.
* Mention Security Cookbook
1. <https://www.ama-assn.org/ama-adopts-principles-promote-safe-effective-mhealth-applications> [↑](#footnote-ref-1)
2. FTC defines “minimal risk” as apps that *only* do one of more of the following: “helping users self-manage their disease or condition without providing specific treatment suggestions; providing users with simple tools to organize and track their health information; providing easy access to information related to health conditions or treatments; helping users document, show or communicate potential medical conditions to health care providers;

automating simple tasks for health care providers; enabling users or providers to interact with Personal Health Records (PHR) or Electronic Health Record (EHR) systems; and transferring, storing, converting format or displaying medical device data, as defined by the FDA’s Medical Device Data Systems regulations.” [↑](#footnote-ref-2)
3. Accessory to a regulated medical device, transforms mobile platform into regulated medical device, or performs sophisticated analysis or interpreting data from another medical device. [↑](#footnote-ref-3)
4. See API Task Force Final Report, <https://www.healthit.gov/facas/sites/faca/files/HITJC_APITF_Recommendations.pdf>, Topic 3 Endorsement/Certification of Apps, page 17. “The Task Force discussed the pros and cons of consumer protection benefits of an app certification process; however, ultimately, we favor a secondary market in app endorsements. In such a market, various kinds of organizations (EHR vendors; security experts; consumer advocacy groups; clinical professional societies; provider organizations) can "endorse" a given app through a distributed, publicly visible process, without centralized regulatory oversight.” [↑](#footnote-ref-4)
5. HIPAA is US-realm-specific, for example purposes only. [↑](#footnote-ref-5)
6. For US Realm, FDA is the regulating agency. See <https://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf>. Section V.A says that the following type of app IS within FDA oversight: “Mobile apps that become a regulated medical device (software) by performing patient-specific analysis and providing patient-specific diagnosis, or treatment recommendations. These types of mobile medical apps are similar to or perform the same function as those types of software devices that have been previously cleared or approved. ”
Appendix B, which contains a list of apps that MAY meet the definition of medical device, for which FDA intends to exercise enforcement discretion. Examples include “Mobile apps that are intended for individuals to log, record, track, evaluate, or make decisions or behavioral suggestions related to developing or maintaining general fitness, health or wellness…” [↑](#footnote-ref-6)
7. “EHR-Integrated” in this example means that the app is designed and developed as part of the EHR application and offered by a provider, i.e., it is not standalone or independent of an EHR. Note that even if the consumer sends data to an EHR, and the EHR accepts the data, that does not in itself make the app developer a business associate of the covered entity (source: Office of Civil Right Health App Use Scenarios and HIPAA) [↑](#footnote-ref-7)
8. The “consumer” and the “patient” are the same person in this example. From the EHR’s perspective, the record is a patient record. [↑](#footnote-ref-8)
9. Note: “Product” is used interchangeably with “App” in cMHAFF conformance statements. Also, “product” is not intended to imply that it is sold commercially: an App is the “work product” of someone developing software for consumer health. [↑](#footnote-ref-9)
10. This means that the EHR is connected to the mobile app, such that the EHR is part of the overall system with which the consumer interacts. [↑](#footnote-ref-10)
11. Also include discussion of where the same terms are used with different meanings in clinical/EHR space [↑](#footnote-ref-11)
12. “Computer” is broadly defined to encompass smart devices such as phones, as well as PCs, servers, and all other computing machinery. [↑](#footnote-ref-12)