**Consumer Mobile Health Application Functional Framework, V 0.3 (DRAFT)**

HL7 International: Mobile Health Work Group

August 18, 2015

**Section 1: Introduction**

As of 2015 there are thousands of consumer health applications (apps) which run on smartphones, 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 primary goals of the HL7 Consumer Mobile Health Application Functional Framework are to provide a standard against which the security and privacy of a smartphone (or tablet) app can be assessed and 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 functionality of an app, but can be extended to do so through the use of profiles developed from the Framework.

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. Chapter Two introduces three exemplary use cases of increasing complexity which have served to guide development of the Framework.

Chapter Three 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 consists 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, which 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”.
* 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 by use case: As applicable, the differential application of conformance criteria by type of app is discussed, referencing the model use cases described in Chapter Two.

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 the 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 provide a path to certification such that apps can promote their conformance so 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.

For the 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 a Draft Standard for Trial Use (DSTU) in 2016.

**Section 2: 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 how app data is connected 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, they are meant to demonstrate a continuum of issues which may be applied to any app.

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 entity.

 

|  |  |
| --- | --- |
|  | **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 an Apple Watch. The app has an ability to download weight, activity, and food consumption information to PHRs through a published API. App developer is not a HIPAA entity, but app can be white-labeled by HIPAA entities.



|  |  |
| --- | --- |
|  | **Device Integrated** |
| **FDA App Categorization** | wellness |
| **FDA Data Device Categorization** | unregulated 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 Disease Management App**

A diabetes management app allows a consumer to collect blood sugar readings through a Bluetooth-enabled glucometer. Activity information is collected through a Fitbit device, 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. 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. From the cloud platform, consumer information is “pushed” to the consumer’s EHR. 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 nurse care manager when a set number of high or low readings are noted within a proscribed period of time. App developer is a HIPAA entity.

 

|  |  |
| --- | --- |
|  | **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 |

**Summary of Major Differences in Use Case Scenarios**

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

**Section 3: Conformance Criteria, Resources, and Implementation Guidance**

**General Considerations**

Conformance Criteria in this section follow a lifecycle model in relation to a consumer’s use of mobile health application, from first finding an app in a smartphone platform’s App Store to disuse and de-installation.

Each section follow a common format. Criteria are separated from “force”. That is, each criteria stated in a neutral way, and the optionality of addressing the criteria while claiming conformance to the standard, is in a separate column. Force follows this convention:

SHALL This criteria is not optional and must be addressed.

SHOULD While not required, this is criteria which are intended to be elevated to SHALL status within the next 3 years and should be given strong consideration in product design and development.

 MAY Best practice which is intended to be elevated to SHALL status within the next 3 years, and which can be considered for included in a product given scope constraints and perceived applicability.

[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.

**Outline of Conformance Sections**

|  |  |
| --- | --- |
| 1. **Product Development and Support**
	1. Regulatory Considerations
	2. Product Risk Assessment and Mitigation
	3. Product Usability
	4. Customer Support
2. **Download and Install App**
	1. App Store Experience
	2. Launch App and Establish User Account
3. **Use App**
	1. User Authentication and Authorization to Access App Services
	2. User Authorizations for Data Collection and Use
	3. Pairing User Accounts with Devices and Data Repositories
	4. Security for Data at Rest
	5. Security for Data in Transit
	6. Data Authenticity, Provenance and Associated Metadata
	7. In-app Payments
	8. Notifications and Alerts
	9. Product Upgrades
	10. Rewards and Incentives
	11. Audit
4. **App Service Termination**
	1. App and Data Removal
	2. Permitted Uses of Data Post Account Closure
 |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |  |
|  |  |  |
|  |  |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| 1. **Product 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 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. **Regulatory Considerations**
 |
| 1 | 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 “medical device” according to the U.S. Food and Drug Administration (FDA), and if so, obtaining necessary pre-market approval. |
| 2 | Shall[IF] | [App requires regulatory approval] Regulatory approval is obtained before app is made available to the general public. |
| ***Regulations, standards, and implementation tools***U.S. Food and Drug Administration: Mobile Medical Applications, <http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm255978.htm> |
| ***Implementation guidance by use case***Use Case A: In the US Realm, a walking app which encourages general wellness is not considered a medical device by the FDA.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, such as a Fitbit, 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. |

|  |
| --- |
| **1.2 Product Risk Assessment and Mitigation** |
| 1 | Shall | Complete a product risk assessment using an established risk management framework. The framework should be one which is used by a Realm’s health systems to determine risk of inappropriate disclosure of medical information. |
| 2 | Shall | 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). |
| 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. |
| 4 | Shall | In development, follow secure coding practices using an established framework. |
| 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. |
| 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. |
| ***Regulations, standards, and implementation tools***National Institute for Standards and Technology (NIST), Cybersecurity Framework, <http://www.nist.gov/cyberframework/> 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> |
| ***Implementation guidance by use case***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. |

|  |
| --- |
| **1.3 Product Usability** |
| 1 | Shall | Assess product against an industry-validated usability assessment tool, using subjects who are demographically-similar to intended users. |
| 2 | Shall | Assess product for usability by people with motor disabilities. |
| 3 | Shall | Assess product for usability by visually-impaired people using a standard mobile screen reader. |
| 4 | 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. |
| 5 | 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.* |
| ***Regulations, standards, and implementation tools***U.S. Department of Health and Human Services, usability.gov, <http://guidelines.usability.gov/>W3C Mobile Usability, <http://www.w3.org/WAI/mobile/>  |
| ***Implementation guidance by use case***These conformance statements apply to any type of app addressed in this standard. Specific usability measures 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.  |

|  |
| --- |
| **1.4 Customer Support**  |
| 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 within two business days. |
| 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 | Customer support responses will include the option for the customer to record that the response is insufficient, which will constitute a new customer support query |
| 7 | Shall | The count and percentages of customer support queries that are deemed insufficient will be reported on a performance dashboard available, at the least, to the application’s customers and its business associates.  |
| 8 | May | The performance dashboard may be publicly available and offer features for comparison with similar or competing apps |
| ***Regulations, standards, and implementation tools***  |
| ***Implementation guidance by use case***The level of customer support should be proportional to the level of health support offered by the app. For example, a general wellness app, like the walking app described in Use Case A may only offer customer support by email with a promised two-day response, while an app providing blood sugar level information with alerts offers one-tap phone support with extended support hours, if not 24/7 availability.(RDG Note: May not belong in this section) The primary purpose of the app is customer benefit. Therefore measuring and transparently reporting customer benefit is the main means of reflecting the continuing value of the app for the app’s continuous improvement and competitive success. |

|  |
| --- |
| 1. **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.The experience of installing an app begins at an app store and completes on a user device |

|  |
| --- |
| **2.1 App Store Experience** |
| 1 | Shall | The payment amount for the app, if any, must be clearly noted according to App Store rules. |
| 2 | Shall | Apps which have required or optional payments after download must clearly state this in the 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). |
| 3 | Shall | The description of an app includes the main functionality of the app. |
| 4 | Shall | Before download, a user can easily access the app’s Terms of Use. This may be accomplished through a link in the app description in the App Store. |
| 5 | Shall | Before download, a use can easily access the app’s Privacy Policy. This may be accomplished through a link in the app description in the App Store. |
| 6 | Shall | Screen shots of the app accurately depict a user’s experience of the app. |
| 7 | Shall[IF] | [App cost is free/subsidized through in-app advertising] In creating targeted advertising, selections are not made based on user data generated by the app. |
| ***Regulations, standards, and implementation tools***[Apple and Android rules for app descriptions in the Apple App Store and Google Play] |
| ***Implementation guidance by use case***Criteria apply equally to all 3 model use cases. |

|  |
| --- |
| **2.2 Launch App and Establish User Account** |
| 1 | Shall | A user can review the app’s Terms of Use before personal data about the user is collected or used. |
| 2 | Shall | User acceptance of the app’s Terms of Use is logged before a user account is created. (See section x.x 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 | Shall | Subject of account is at least 13 years old or is under the age of 13 years and has documented approval from a parent or guardian to establish an account. |
| 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;
2. 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 | Should[IF] | [Access to account exposes PHI or PII] The user is given an option to utilize strong authentication methods (e.g., multi-factor authentication) 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. |
| ***Regulations, standards, and implementation tools***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> National Institute of Standards and Technology, Electronic Authentication Guideline, NIST 800-63-2. |
| ***Implementation guidance by use case*** 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. |

|  |
| --- |
| 1. **Use App**
 |
| The functionality of an app, its sponsorship, and linkages to external data sources all effect 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.  |

|  |
| --- |
| **3.1 User Authentication and Authorization to Access App Services** |
| 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.  |
| 3 | 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. |
| 4 | Shall[IF] | [EHR is a system actor] 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. |
| 5 | Shall | At the request of an app user, the app terminates such that access to PHI or PII requires a new, successful authentication attempt. |
| 6 | Should | The app terminates access to PHI or PII after a period of time as described in the app’s Terms of Use. 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.  |
| 7 | Shall[IF] | [EHR is a system actor] The app terminates access to PHI or PII after a period of time as described in the app’s Terms of Use. |
| ***Regulations, standards, and implementation tools***National Institute for Standards and Technology (NIST), Cybersecurity Framework, <http://www.nist.gov/cyberframework/>  |
| ***Implementation guidance by use case*** See section 2.2 for a discussion as to the selection and ongoing use of a user authentication mechanism. |

|  |
| --- |
| **3.2 User Authorizations for Data Collection and Use** |
| 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. |
| 3 | 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 or data source 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 and calendars. |
| 4 | 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. Permission is requested before the first potential transmission of data. Permission is re-requested before any additional data elements are sent to an external data source when permission had previously been extended. |
| 5 | 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. |
| 6 | Shall[IF] | [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. |
| 7 | 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. |
| 8 | 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. |
| 9 | 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. |
|  |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.3 Pairing User Accounts with Devices and Data Repositories** |
| 1 | Shall | User has authenticated identity to an app and has an active session before pairing an external device to an app account. |
| 3 | Shall | Before a device is paired with an individual known by the app, 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. |
| 4 | 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. |
| 5 | Shall | Before a device is paired with an individual known by the app, 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. |
| 6 | Shall | [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. |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.4 Security for Data at Rest** |
| 1 | SHALL | PHI and PII stored on a smartphone is stored as encrypted values. |
| 3 | SHALL | PHI and PII stored on any external server is stored as encrypted values. |
| 4 | 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. |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.4 Security for Data at Rest** |
| 1 |  | PHI and PII stored on a smartphone is stored as encrypted values. |
| 3 | SHALL | PHI and PII stored on any external server is stored as encrypted values. |
| 4 |  | 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. |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.5 Security for Data in Transit** |
| 1 | SHALL | PHI and PII transmitted between an app and an external data source, including data generated through a device associated with the app, is transmitted as encrypted values. |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.5 Security for Data in Transit** |
| 1 |  | PHI and PII transmitted between an app and an external data source, including data generated through a device associated with the app, is transmitted as encrypted values. |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.6 Data Authenticity, Provenance and Associated Metadata** |
| 1 | SHALL | Apps conform to Best Practices for Data Authenticity, Provenance, and Associated Metadata (This will require an Appendix and a testing reference such as Drummond Group?) |
| 3 | 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. |
| 4 | 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. |
| 5 | SHALL[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. |
| 6 |  | (Others to follow if not deemed too much of a reach…) |
| 7 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.7 In-app Payments** |
| 1 | Shall | In-app payments are not required in order for the app to provide its main functions. |
| 2 | 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. |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.8 Notifications and Alerts** |
| 1 | Shall | Opt-in consent is required by the account holder before receiving notifications and alerts from an app. |
| 3 | 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. |
| 4 | Shall | An account holder can change consent decisions about notifications and alerts through settings available on the smartphone on which the app was downloaded. |
| 5 | Shall | As permitted by the account holder, notifications and alerts may be sent to the account holder or to another person or entity. |
| 6 | Shall | Notifications and alerts contain the least amount of information necessary for the recipient of the alert to take a focused action. |
| 7 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.9 Product Upgrades** |
| 1 | Shall | The app respects operating system level permissions concerning automatic product updates. |
| 3 | Shall | 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 |
| 4 | 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.  |
| 5 | 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. |
| 6 |  |  |
| 7 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.10 Rewards and Incentives**  |
| 1 | Should | Completion of activities while using the app results in the app user receiving a tangible or intangible reward. |
| 3 | Shall[IF] | [rewards are given for app participation] Once given, rewards are not withdrawn. |
| 4 | Shall[IF] | [rewards are given for app participation] A promised reward which is used as an incentive to complete app activities must be promptly fulfilled when the app user has completed the activities. If the reward is not given immediately, a time limit by when the reward will be given is clearly stated. |
| 5 | May | A set of smaller rewards can be accumulated into a greater reward (that is more valuable than the sum of its parts). This approach makes it easier and less expensive for the rewarder to manage – by manufacturing, delivering, and governing a single reward as opposed to multiple smaller rewards.  |
| 6 | May | A reward can be donated to another party (either by naming a specific recipient – or by selecting a category of recipient (e.g., a homeless child under age four, or an Army veteran). Such donations can be a form of drawing other app users to the app; consider that a social group can effectively “purchase” an expensive item for a targeted individual (e.g., purchase a wheelchair for a child) by pooling their rewards. |
| 7 | May | The recipient of a donated reward can return a “Thank You” to the folks who contributed to a forwarded reward (a donation). |
| 8 | Shall | Awards and incentives must be governed in order to reduce fraud and abuse. |
| 9 | May | Information regarding the selection of a certain reward can be valuable (salable) to the marketing department of manufacturers (Note: “secondary use” of heath data needs to be well-thought through!) “Badging” or “Guru-Status Icon” status. |
| 10 | Should | A social group can use an app in real-time to identify and fulfill a targeted health need (e.g., We now only need 8 more people to hand out blankets to homeless people on Saturday night on Oak Street.) |
| 11 | Shall | If a forwarded reward is rejected (or fails to reach its target), the reward returns to the original donor (and the donor is notified of the returned reward). |
|  |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **3.11 Audit** |
| 1 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| 1. **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. |

|  |
| --- |
| **4.1 App and Data Removal** |
| 1 | Shall | An app Account Holder can remove an app from a smartphone at any time. |
| 3 | 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. |
| 4 | Shall | An app Account Holder can close an associated account or data store associated with the app. |
| 5 | 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. |
| 6 | 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. |
| 7 | 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. |
| 8 | Shall | 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. |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |

|  |
| --- |
| **4.2 Permitted Uses of Data Post Account Closure** |
| 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. |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| ***Regulations, standards, and implementation tools*** |
| ***Implementation guidance by use case*** Use Case A: Use Case B:  Use Case C: |