Xcertia™

mHealth App Guidelines

2019 Board Approved Xcertia Guidelines

Issued on: August 12, 2019

The Xcertia Guidelines History

Today's Xcertia Guidelines were first conceived in 2012. As part of the development process, a panel comprised of thought leaders in the healthcare industry such as the Association of American Medical Colleges, Mobile Marketing Association, Healthcare Information and Management Systems Society (HIMSS), the U.S. Food and Drug Administration (FDA), and other federal agencies, was formed. In the spirit of collaboration, and to seek public input, these guidelines were published for review and comment to maximize public and interested parties' input.

In 2015 those same guidelines were updated with input from subject matter experts in the key areas of Operability, Privacy, Security and Content. Shortly thereafter these guidelines were transferred to the newly formed non-profit.

Today, these guidelines now known as the Xcertia Guidelines, are backed by its founding members, the American Medical Association (AMA), the American Heart Association (AHA), HIMSS, and the DHX Group, with a shared purpose to provide a level of assurance to clinicians and consumers alike, that the mobile health apps that comply with the guidelines are vetted to deliver value to the end user.

Under the Xcertia watch, the guidelines were updated in 2017 and then posted on the Xcertia website for public comment. At the Connected Health Conference 2018 the Privacy and Security sections of the guidelines were again updated and issued for public comment following that update by the Xcertia Work Groups in these two disciplines.

In February of 2019 the Xcertia Guidelines will have gone through a complete review and editing process by the organization's various work groups. These groups consisted of over forty individuals and contained subject matter experts from a number of healthcare organizations and disciplines with expertise in the various sections within the guidelines. As part of that effort the Xcertia Guidelines are divided into five sections, Privacy, Security, Usability, Operability and Content, reflecting the key areas of guidance to ensure mHealth apps deliver true value in a trusted environment to improve product adoption and use.

Since their release in February of 2019 the guidelines were available for public comment up until May 15, 2019. Those comments have been considered by the work group leaders and their teams and where appropriate incorporated into the Final 2019 Version of the Xcertia Guidelines.

App Privacy Guidelines

App Privacy (P) Guidelines

Privacy will assess whether a mobile health app protects the user's information, including Protected Health Information (PHI), Personal Information (PI), Personally Identifiable Information (PII) in full compliance with all applicable laws, rules and regulations. Where jurisdictions may conflict, the App Designer shall comply with the more rigorous requirements. It is incumbent upon the developer to understand the scope and full requirements of the Privacy Rules and potential notification requirements of the region(s) for which they intend to operate. Developers should have relevant procedures in place and be able to document those procedures.

Guideline P1 – Notice of Use and Disclosure

The Privacy Notice is externally facing and describes to an app user how the organization collects, uses, and retains their data (e.g., PHI, PI, PII). This notice should be unbundled from other information notices regarding the application. The type(s) of data that the app obtains, and how and by whom that information is used, is disclosed to the user in a Privacy Notice

Requirements for Guideline P1

- P1.01 Access: The identity of any entities that will have access to, collect and/or use of the user's personal information, shall be made available and disclosed to the user on an at least an annual basis and shall disclose use by any parties as a part of the use chain.
- P1.02 Usage: The app publisher shall disclose any and all ownership, rights or licenses to any data collected about the app and its usage, including the use of any data for commercial purposes.
- P1.03 Material Changes to Use: The app shall have a section (tab, button or equivalent) or active link to its Privacy Policy, and owner represents that commercially reasonable efforts are used to notify users of any material changes to its Privacy Policy.
- P1.04 User Registration: If registration is required to use all or some of the app's features, the user shall be provided with an explanation as to the uses of the registration information.
- P1.05 Data Collected and Opt Out: User shall be provided (or have access to) a clear list of all data points collected and/or accessed by the app, including by the app publisher and all third parties such as in-app advertisers. This includes personal data pertaining to the usage of the app, including but not limited to browsing history, device

(e.g., unique identifiers), operating system, and IP addresses. How and from where such data points are collected shall be disclosed. An Option should exist for user to opt-out of passing data to in-app advertisers.

- P1.06 Data Collected and Disclosed: User shall be provided (or has access to) a clear list of all data points collected and/or accessed by the app pertaining to the specific user, including user-generated data and data that are collected automatically about the user through other means or technologies of the app. This includes data points collected for the purpose of any third-party sharing. How and from where such data points are collected is disclosed.
- P1.07 Affirmative Consent to Use Data: The app publisher shall obtain affirmative express consent before using user data in a materially different manner than was previously disclosed when collecting the data or collecting new data, including for third-party sharing.
- P1.08 Affirmative Consent to Collect Data: The app publisher shall obtain affirmative express consent before collecting personal data, in particular, Personally Identifiable Information (PII), Personal Health Information (PHI), financial data or location data, including obtaining HIPAA authorizations where applicable.
- P1.09 Use and Updates of Information: The privacy policy shall inform users how they can get a copy of their personal information that was collected by the app. A designated individual or toll-free number may be required to be listed depending on domicile of user. The privacy policy shall also inform users how they can correct and update information supplied by, or collected about them, held by or on behalf of the owner, or shared with third parties, including the identity of such third parties, particularly in compliance with the HIPAA Privacy Rule, if applicable, and any other state or
- international laws, rules, or regulations to the extent applicable.
- P1.10 Do Not Track Mechanism: If not otherwise provided by default, the app shall allow users to control the collection and use of their in-app browsing data by supporting an online Do Not Track mechanism.
- P1.11 Opt Out or Do Not Contact: If not otherwise provided by default, the app shall allow users to control their receipt of commercial messages from the app publisher and third parties through an "opt out" option, "do not contact," or substantially similar feature.
- P1.12 Sharing of Data: The app publisher shall not share any personal data with third parties, unless the app publisher: (i) has an agreement with such third party that addresses safeguarding any and all such user data (BAA); and (ii) takes the necessary measures to anonymize/de-identify all user data in accordance with the Health and Human Services Safe Harbor guidelines for de-identification.(iii) the user provides an affirmative user consent (iv) except when expressly disclaimed by app publisher (v) The app publisher has documented this within the Privacy Policy.

- P1.13 User Ability to Delete Data/Accounts: App publisher should allow a user to delete all personal data from systems if canceling or deleting accounts. This functionality could be accessed by the user in app or by app owner.
- P1. 14 Changes to Privacy Policy: A mechanism shall be in place to notify users of changes to the Privacy Policy.
- P1.15 Consent to Changes in Privacy Policy: A mechanism shall be provided that enables users to acknowledge and consent to changes to the Privacy Policy.
- P1.16 Notification in Event of Breach: User will be promptly notified (according to state or federal laws or contractual obligations) if breach occurs that has compromised their information in accordance with applicable state, federal and country laws.

Guideline P2 - Retention

If data is collected, the user shall be informed about how long the data is retained.

Requirements for Guideline P2

- P2.01 The Privacy Policy shall disclose the retention policy regarding user information. Such statement shall include policies with respect to data retention under any third-party data sharing arrangement.
- P2.02 Retention and deletion time periods, which are based on clearly defined business needs or legal obligations, shall be set. If business needs are defined as "in perpetuity," this shall also be disclosed.

Guideline P3 – Access Mechanisms

The app user is informed, through an End User License Agreement, if the app accesses local resources (e.g., device address book, mobile and/or LAN network interface, system stored credit card information, GPS and other location-based services, contacts, camera, photos, SMS or MMS messaging, and Bluetooth) or resources from and/or for social networking platforms, provided with an explanation by any appropriate means (e.g., the "About" section) as to how and why such resources are used, and opt-in consent is obtained to access such resources.

Requirements for Guideline P3

- P3.01 If the app accesses any of the mobile device's native hardware (camera, microphone, GPS/location, Calendar, Address Book, etc.) the express reason for requiring such access shall be disclosed to the user, separate from any warning/consent present in the mobile operating system.

- P3.02 If the app accesses or uses any Wi-Fi, LAN, or mobile network data connections, an estimate of the amount of data consumed shall be provided to the user along with a notice that carrier data charges may apply.
- P3.03 If the app accesses social networking sites (such as Facebook, Instagram, or like social media), the reason why such sites are being accessed is disclosed to the user.

Guideline P4 - Health Insurance Portability and Accountability Act (HIPAA) Entity or Business Associate

If the app, on behalf of a Covered Entity or a Business Associate (each as defined by HIPAA and the rules thereunder), collects, stores, and/or transmits information that constitutes Protected Health Information (as defined by HIPAA and the rules thereunder), it does so in full compliance with HIPAA and all applicable state and international laws, rules and regulations.

Requirements for Guideline P4

- P4.01 The user can affirmatively opt in or out (at any time) of information shared with or given access by third parties.
- P4.02 The app publisher certifies that a Business Associate Agreement (BAA) has been executed pursuant to HIPAA with any and all necessary third parties.
- P4.03 The user can access or request any of his/her Protected Health Information (PHI) collected, stored and/or transmitted by the app.
- P4.04 The app publisher uses requisite efforts to limit the use and disclosure of PHI, including ePHI, to the minimum necessary to accomplish the intended purpose (e.g., “need-to- know”).
- P4.05 The publisher must demonstrate that procedures are in place so that in the event of a breach the app publisher shall notify affected individuals, HHS, and in some cases, the media (news agencies, print, radio, etc.) of a breach of unsecured PHI. Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach.

Guideline P5 – Children’s Online Privacy Protection Act (COPPA)

The app has measures in place to protect children in accordance with applicable laws and regulations if website is directed at children (see specific guidance Children’s Online Privacy Protection Act).

Requirements for Guideline P5

- P5.01 The app provides clear notice of the content that will be made available and its suitability for specific age groups.
- P5.02 The app includes a clear and conspicuous Privacy Notice/Policy that addresses use by any child under the age of 13 and prevents usage without verifiable parental authority (please note state laws may have additional carve out regulations for children).
- P5.03 The app provides for an age verification process—either automatic or self-reported—to control access to age-restricted content and to minimize the inappropriate collection, use, or disclosure of personal information from a child.
- P5.04 The app does not, without obtaining verifiable parental/legal guardian consent, collect, use, or disclose data from any child under the age of 13.
- P5.05 The app enables a parent/legal guardian who becomes aware that the child has provided information without his/her consent to contact the app publisher and eliminate account/delete that data.
- P5.06 The Privacy Policy provides that the app publisher will delete any child's personal information upon notice, or if the App publisher becomes aware or has knowledge, that such information was provided without the consent of a parent/legal guardian, including information that was shared with a third party.
- P5.07 Apps that are intended for children must have a location default setting that enables parents/legal guardians to prevent the app from automatically publishing their child's location.
- P5.08 Apps that are directed at children under the age of 13 will have a default setting that prevents in-app purchases.
- P5.09 Apps that are directed at children under the age of 13 will have a default setting that prevents usage of camera and microphone.

Guideline P6 - General Data Protection Regulation (GDPR)

The app has measures in place to comply with applicable laws and regulations related to the European Union General Data Protection Regulation (GDPR).

Requirements for Guideline P6

- P6.01 Provide Privacy Notice at the time user is providing information to the app. The Privacy Notice should be available in search feature.

- P6.02 The Privacy Notice must be concise (plain language), transparent and accessible. For the Privacy Notice to be easily readable, key information is at front of notice and in a layered notice approach links are available for additional information in full version.
- P6.03 The Privacy Notice must include the name of the organization, processor, name and contact details of the representative, and contact details of the Data Protection Officer (DPO) if a DPO is required.
- P6.04 The Privacy Notice must state the lawful basis, legitimate purposes, and rights available to individuals in respect of processing.
- P6.05 The user must be informed of the categories/source of personal data obtained if it is obtained from third party sources. *This must be provided within a reasonable period of obtaining the personal data and no later than one month. Notice must be provided of the recipients of categories of personal data, whether the individuals are under a statutory or contractual obligation to provide personal data and the details of transfers of personal data to any third countries or international organizations.*
- P6.06 The details and existence of automated decision-making including profiling (if applicable) and the retention periods for personal data must be provided.
- P6.07 Unexpected uses of user data should be posted on the front page of the Privacy Notice and there must be separate consent for different uses. A user must be given a simple way to consent to all types of uses listed (e.g. opt in/opt out boxes for each). If the app is requesting the user to receive direct marketing materials, then there should be a separate opt out box.
- P6.08 The user must be put on notice that they have the right to withdraw from further use of data (if applicable through respective regional data governance laws) and the right to file a complaint with the respective regional supervisory authority.
- P6.09 Best practice is to conduct audits to see what personal information the app maintains and conduct user testing to see if the privacy notice is easily understandable.
- P6.10 The app developer must ensure the Privacy Notice is consistent with current use. If a material change is made to the collection or use of data, the Privacy Notice must updated prior to processing.
- P6.11 If the event of a breach of personal data, understand the type of data that has been impacted. Prepare a written report. And, based upon notice requirements of area of operation, Report within 72 hours of becoming aware of the reportable breach to the relevant supervisory authority.
- P6.12 The App Developer shall be responsible for knowing relevant and appropriate regulations for the Regions in which they intend to operate

- P6.13 The End User Licensing Agreement (EULA) should document how notice shall be provided to individual and appropriate authorities.

References: Additional information may be found at these sites:

US State Breach Notification Requirements: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

European Union General Data Protection Requirements- Information Commissioners Office UK: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed

Health and Human Services Safe Harbor: https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=90f45f0c857144405b17a43c35600c16&ty=HTML&h=L&mc=true&r=SECTION&n=se42.5.1001_1952

HIPAA: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html?language=en

App Security Guidelines

App Security (S) Guidelines

The Security Guidelines will assess if the application is protected from external threats and maintain the integrity, availability, confidentiality, and resilience of the data.

Guideline S1 – Security Operations

The app publisher ensures that the app's security procedures comply at all times with generally recognized best practices and applicable rules and regulations for jurisdiction(s) in which the app is intended to be sold or used and such procedures are explained or made available to users.

Requirements for Guideline S1

- S1.01 Administrative, physical, and technical safeguards to protect user's information from unauthorized disclosure or access are provided and employed.
- S1.02 Access to user's information is limited to those authorized employees or contractors who need to know the information in order to operate, maintain, develop, or improve the app.
- S1.03 If the app utilizes unique identifiers, the identifier is linked to the correct user and is not shared with third parties.
- S1.04 If any third-party vendor services are utilized as part of the app, an information security risk assessment should be conducted of the respective third parties.
- S1.05 If your organization is subject to HIPAA or other Information Security and/or Privacy regulations, an internal risk assessment for any systems related to PHI/PII should be conducted.
- S1.06 App publisher should create and maintain a baseline configuration document for potential risks to be identified.
- S1.07 Risk-appropriate authentication methods are used to authenticate users.
- S1.08 A written description of security procedures is provided in a section of the app (tab, button, or equivalent) or through an active link. The security procedures are written in clear, easy-to-understand language and terms and are affirmatively agreed to by the user. Such components include, but are not limited to, how personal information is safeguarded, how unique identifiers are linked to the correct user, and authentication methods used.

- S1.09 App publisher should designate someone to be responsible for information security.
- S1.10 App publisher staff designated for information security should have a baseline of information security knowledge.
- S1.11 Responsibilities for information security staff should be clearly documented.
- S1.12 Any staff members handling PHI/PII should be required to take Information Security Awareness training, highlighting HIPAA.
- S1.13 The app publisher has a mechanism in place to review security procedures on an ongoing basis and update security procedures, as necessary, to ensure that they comply at all times with applicable rules and regulations for jurisdiction(s) in which the app is intended to be sold or used.
- S1.14 Cloud-based apps meet Statement on Guidelines for Attestation Engagements (SSAE) No. 16 requirements and a SSAE No. 16 audit report is provided. (http://ssae16.com/SSAE16_overview.html)
- S1.15 If the app uses Short Messaging Service (SMS) or Multi-Media Message Service (MMS), the user is informed whether messages are encrypted and, if so, the level of encryption.
- S1.16 Any app that collects, stores and/or transmits user financial data for any purpose, including payment processing, or the app directs to any website for the purpose of collecting and/or processing of financial information, including any third-party website, shall comply with all applicable Federal and state laws, rules and regulations, and private sector regulatory best practices guidelines and initiatives regarding data security requirements.

Guideline S2 – Vulnerability Management

The app, including without limitation, any advertisement displayed or supported through the app, is free from known malicious code or software such as malware, including, but not limited to, viruses, worms, trojan horses, spyware, adware, rootkits, backdoors, keystroke loggers, and/or botnets at time of release and/or upgrades.

Requirements for Guideline S2

- S2.01 A scan of the app by the app developer using scanning software does not reveal any known malicious code or software objects prior to release.
- S2.02 A scan of any third-party code, including advertising networks, incorporated into app for purposes of displaying or supporting advertisements (e.g., banner, interstitial) does not reveal any known malicious code or software.

- S2.03 If ongoing scanning does produce evidence of malicious code or software objects, proactively work to update the app and notify end users.

Guideline S3 – Systems & Communication Protection

If the app collects, stores or transmits any personal data, including, but not limited to, usernames and passwords, such information is collected, stored, and transmitted using encryption.

Requirements for Guideline S3

S3.01 Passwords are stored using a random length, , one-way salted hash, or current accepted guideline.

- S3.02 Usernames and passwords are collected and transmitted only when using encryption between the client app and the server.
- S3.03 Other personal information while at rest and/or in motion is encrypted using a generally recognized, industry-accepted encryption method (e.g., FIPS 140-2, ISO/IEC) for such information and the encryption level is disclosed.
- S3.04 App contains security safeguards to verify the identity of intended user in the event of forgotten, lost or unknown user name, password and/or passcode ("unique identifiers"), for purposes of reminders, re-linking, or creation of new unique identifiers.
- S3.05 Organization should have a change management process when changes are made to the app or critical systems in operability check there and if okay delete from here.
- S3.06 Information systems related to the app should have antivirus software and mechanism to keep application environment up to date with security patches.
- S3.07 Application data should be backed up regularly.
- S3.08 Firewalls should be used for internal and external connections.
- S3.09 Vulnerability assessments should be conducted on the application and organizational network on a regular basis.
- S3.10 If removable media is used for the storage of personal data, the media should be encrypted to protect the data from unauthorized access.

- S3.11 Organization should have a documented patch management process for systems and app.
- S3.12 Installed App and respective infrastructure should have the capability to log and audit activity within the system, e.g. who did what, when and how.
- S3.13 Installed App Audit logs should be maintained for a minimum of 90 days.

Guideline S4 – Compliance

If the app collects, stores or transmits information that constitutes PHI as defined by HIPAA and the rules thereunder (e.g., app publisher constitutes a Business Associate pursuant to HIPAA), it uses requisite efforts to maintain and protect the confidentiality, integrity, and availability of individually identifiable health information that is in electronic form (e.g., ePHI).

Requirements for Guideline S4

- S4.01 If the app, or through its use, subjects the user or any party to HIPAA, the app publisher has implemented administrative, physical and technical safeguards, and developed policies and procedures, pursuant to the HIPAA Security Rule, as applicable. For purposes of the technical safeguards/security controls, only certain certified encryption technologies are permissible for compliance with HIPAA.
- S4.02 If applicable, the app or the app publisher has safeguards in place or uses requisite efforts to comply with all obligations pursuant to any BAA, including capabilities to assist a covered entity in curing any breach, and address all other requirements of HIPAA in the event of a breach including notifying affected users.
- S4.03 The app publisher has the capabilities to enable compliance, and shall comply with any and all applicable notification requirements to its users in the event that users' PHI is or is suspected to be compromised (e.g., Breach Notification Rule pursuant to HIPAA including the capability to support and execute notification requirements).

  S4.04 The app publisher has a mechanism to notify end users about apps that are banned or recalled by the app publisher or any regulatory entity (e.g., FDA, FTC, FCC, UL).
- S4.05 In the event that an app is banned or recalled, a mechanism or process is in place to notify all users about the ban or recall and render the app inoperable.
- S4.06 If the app constitutes a medical device (e.g., 510(k)) or is regulated by the FDA in any other capacity, the app publisher has a policy and a mechanism in place to comply with all applicable rules and regulations for purposes of handling all aspects of a product notification or recall, including all corrections and removals.

Guideline S5 – Access Control and Authentication

If the app collects, stores and/or transmits personal information, the app offers one or more industry-accepted methods for guarding against identity theft.

Requirements for Guideline S5

- S5.01 The app provides a method for securely authenticating the user at a session level (e.g., password, pass phrase, PIN, challenge phrase) and utilizes additional methods or techniques to further secure the identity of the users whenever the system is initially establishing identity, or the system has indications that the identity might have been compromised (e.g., multiple password failures).
- S5.02 Unique user IDs should be used for access to all functions within the application.
- S5.03 Access within the application should be limited to what is needed for that individual's specific role.
- S5.04 A process for provisioning and deprovisioning access in a timely fashion should be documented.
- S5.05 For remote access or privileged access should require two factor authentication to reduce the risk of unauthorized access.

Guideline S6 – Asset Management

If the app collects, stores and or transmits personal information, the app maintains a methodology for documenting those Assets.

Requirements for Guideline S6

- S6.01 Organization should have a process for tracking information and physical assets.
- S6.02 Information assets should be classified based upon value to the organizations and outside regulations, e.g. public, internal confidential, sensitive.

Guideline S7 – Physical & Environmental Security

If the app collects, stores or transmits personal information, the app the app publisher shall maintain a record of how Security is maintained.

Requirements for Guideline S7

- S7.01 Organization should have a physical security program.
- S7.02 Physical security program should include security and environmental controls for the building/data center which contains information assets and system.

Guideline S8 – Incident Response

If the app collects, stores or transmits personal information, the app publisher shall create and maintain an Incident Response system.

Requirements for Guideline S8

- S8.01 Organization should have an incident response plan in the event of an information security incident.
- S8.02 If breach is determined, the organization should notify customers and individuals affected in accordance with applicable regulation.

Guideline S9 – Disaster Recovery & Business Continuity

If the app collects, stores or transmits personal information, the app publisher shall provide a documented plan when the app, data or access is not available for use.

Requirements for Guideline S9

- S9.01 Organization should have a documented DR/BC plan in the event that the application, data, or its infrastructure is not available for use.
- S9.02 Tests from data back-up should happen on a regular basis.
- S9.03 Tests of the DR/BC plan should happen on a regular basis.

Content Guidelines

Content guidelines will assess whether the information provided in the application is current and accurate.

Guideline C1 Credible Information Sources

The app is based on one or more credible information sources including, but not limited to: protocols, published guidelines, evidence-based practice and peer-reviewed journals. Appendix 2 provides a selected number of accepted condition specific guidelines.

Requirements for Guideline C1

- C1.01 The app should specify the source of content with documentation. Is it based on content from a recognized source (e.g., guidelines from a public or private entity) with, and documentation (e.g., link to journal article, medical textbook citation) about the information source and copyright compliance is provided. The source should point to current and accepted protocols and guidelines. Additionally, the content within the application should align and not deviate from the referenced source.

- C1.02 If the app is based on content other than from a recognized source, documentation about how and when the content was formulated is provided, including information regarding its relevancy and reliability.

- C1.03 If a previous version of an app or its content becomes medically dangerous due to updated current medical guidelines, the app publisher has a documented process and annual review period or mechanism to update or retract the outdated content version and notify users.

Guideline C2 Current Information

The app's content reflects up-to-date information.

Requirements for Guideline C2

- C2.01 Documentation about the source of the app's content and explanation as to why it is deemed to be up-to-date is provided.

- C2.02 The date(s)/source(s) of the app's content is provided through an "About" section (tab, button or equivalent).

- C2.03 The app publisher has a method or protocol for determining if an app's content requires updating to remain up-to-date. The app publisher will provide an annual review schedule to ensure that content contained in the app is up to date.

- C2.04 The app publisher has a method or protocol for updating the app's content when new or changing information warrants. Updates should include a description of and documentation for each change and be made readily available for app users to identify the timing up these updates.

- C2.05 Any significant deviations in an app's content from the original source (e.g., excerpts, abbreviated versions) are indicated and explained.

Guideline C3 Information Accuracy

The app's description and content are truthful, fair, and not misleading.

Requirements for Guideline C3

- C3.01 documentation is provided to substantiate any claims made in the description and/or content.

- C3.02 Disclosures are provided, as needed, to prevent deception. Such disclosures shall be presented in a clear and conspicuous manner.

- C3.03 Disclosures are provided, as needed, if the app requires an additional fee(s) (e.g., subscription fee) in order to fully access the app, its associated functionality, and/or content.

Guideline C4 Accuracy of Results

An app that contains tools that perform user or patient management functions, including but not limited to, mathematical formulae, calculations, data tracking, reminders, timers, measurements, or other such functions, does so with consistent accuracy and reliability to the degree specified in the app.

Requirements for Guideline C4

- C4.01 When operated, the app produces consistent and accurate results that are independently verifiable.

- C4.02 The app publisher will provide the accuracy and reliability of any calculations in product documentation. Product documentation will also include appropriate sources that support the validity of calculations, measures and other functions

Guideline C5 Advertising Within the App

An app that contains advertisements clearly identifies the advertising and complies with all applicable regulatory requirements, particularly advertisements that involve or relate to products or services that are clinical or related to health.

Requirements for Guideline C5

- C5.01 Information in any app that constitutes advertising is denoted by the message "This is an advertisement" or equivalent legibly displayed next to the advertisement or clearly super-imposed on the actual ad or advertorial..
- C5.02 Information in any app that constitutes advertising will always comply with all applicable regulatory requirements related to the marketing of any product or service, including, but not limited to those of the FDA,

FTC, FCC, and any laws, rules, regulations and policies of other regulatory entities in all jurisdictions that app's owner makes its product available.

- Advertisements should be placed within the app in such a manner as to not create confusion or uncertainty as to what is advertising vs educational information.
- C5.03 App publisher takes commercially reasonable efforts to clearly and prominently indicate (e.g., in the "About" section) that any advertisement, which may be perceived as health care or medical advice or treatment, is being displayed for the sole purpose of advertising and should not be construed as a substitute for medical or clinical advice.

Guideline C6 Documentation of Evidence

The level of evidence and quality of evidence for an app should be transparent and visible to users and health professionals.

Requirements for Guideline C6

* C6.01 The app's public description should clearly state which type of research has been performed to validate its content. These can include the following levels of research:

I. Systematic review or meta-analysis of randomized control trials
II. Randomized control trial/s (number of trials if more than one)
III. Quasi-experimental study
IV. Case-control or cohort studies
V. Systematic reviews of descriptive and qualitative studies
VI. Single descriptive or qualitative study
VII. Expert medical or academic opinion

- C6.02 If level of research performed on the opinion is based on expert or academic opinion (VII) or no study, the app's public description should clearly state, "The effectiveness of the app has not been studied".

- C6.03 If a study was performed, documentation should clearly state who performed such study (C7.01) and whether the study was performed by an independent entity. Furthermore, the app's documentation should state if the study has been published in a peer-reviewed journal, and if so, include the date and the title for both the journal and article. App's documentation should also state any ownership that the study authors (C7.01) have in the solution company, its partners or investors, either currently or at the time the study was performed.

- C6.04 If a study was performed, documentation should state the exposure environment (e.g. hospital, home, community health center, etc.). It should also state the demographics, socioeconomic status, IT literacy, rural/urban, and type/stage of illness of study participants. The relevance of these characteristics to app's goals should be explained.

Guideline C7 Transparency of Evidence

The basis of evidence in literature for the app and the app's design should be transparent and visible to users and health professionals.

Requirements for Guideline C7

- C7.01 App documentation should state whether the app is based upon the results of a study/studies published in peer-reviewed journals. This can include studies of non-digital health interventions that have inspired solution designs. If based on peer-reviewed publications, documentation should state that the app is "informed by the independent study of a separate intervention in a peer-reviewed journal" and include the date and the title for both the journal and article. This statement is in addition to, not replacement, of the preceding statement of which type of research has been specifically performed on the app.

Given that literature reviews are significantly less costly than performing studies,

- C7.02 Documentation should state whether such study authors (C7.01) have had any cooperation with the app publisher, and whether the study authors provide any active input on the app. App documentation should also state any financial relationships that are planned, exist or have existed between such study authors (C8.01) and the app publisher, its partners or investors.

- C7.03 If an app is based on peer-reviewed literature, the documentation should state what type of user research was performed to adapt the literature and solution to the needs of the target user. This could include, but is not limited to design research, human centered design, formative research, user centered design, and co-creation with users. This type of qualitative research can complement and translate quantitative research, but it should not be presented as a replacement for quantitative research.

Guideline C8 Publishing Outcomes Data

The types of results achieved by the app or study of the app should be transparent and visible to users and health professionals.

Requirements for Guideline C8

- C8.01 Documentation should clearly state what metric or indicator is used in studies and claimed to be accomplished by the application. This can include the following type of indicators:

I. Health outcomes
II. Biological outcomes
III. Health behavior outcomes
IV. Online analytics or online behavior outcomes

If the cited indicator is only an online outcome (IV), documentation should clearly state that results do not include "tangible outcomes in health behavior or health outcomes".

- C8.02 The public source of the metric definition should be cited in the app's documentation. This could include a health association, peer-reviewed journal, health standards body.

Guideline C9 Transparency of Data

The context of the app and data should be clear to users and health professionals.

Requirements for Guideline C9

- C9.01 The app's public description should accurately state in plain language what type of individual health data is collected by the app, who it is shared with, and what it used for. This description should specify whether this data is sold to app publisher's partners.
-
- C9.02 App documentation should specify in which types of environments it is designed to operate for all relevant users (e.g. hospital, home, community health center, etc.). This description should explain how the app has been designed to operate in this environment with the minimum burden.

  For further information and guidance, refer to "How to Make Effective Disclosures in Digital Advertising," Federal Trade Commission. (https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf)

Usability Guidelines

App Usability (U) Guidelines

The Usability Guidelines assess how a mobile health app is designed to be safe and easy to use by incorporating five key quality aspects of usability: learnability, efficiency, memorability, prevention of errors, and user satisfaction. Apps designed based on sound usability principles will be optimized for use by the intended users within the intended use environments.

Guideline U1 Visual Design

Apps should follow standards of visual design that promote legibility, clarity of content, and user engagement without introducing unnecessary distraction. Apps that leverage user expectations in their design strategy shorten the learning curve and decrease user frustration.

Performance Requirements for Guideline U1

- U1.01 App layout should be adaptable such that usability and functionality do not differ between landscape or portrait mode. Ideally, interfaces should be flexible to operate in both orientations.
- U1.02 Readability and meaning of content within the app should be consistent across a variety of mobile screen sizes and operating systems.
- U1.03 Contrasting colors should be utilized to help users distinguish between the different elements on the screen, with an emphasis on contrast between the screen background and content (i.e., text and graphics).
- U1.04 Multiple redundant identifiers should be used to indicate critical or safety-related information. Cues can include color, iconography, labeling, or other text.
- U1.05 Extraneous text, graphics, and animation should be used sparingly. Information that is actively populating should serve a purpose and avoid distracting the user or cluttering the screen if only for aesthetic purposes.
- U1.06 Elements critical to app functionality and content understandability should be positioned above the scroll line to minimize the opportunity for missed information. Users should be able to clearly identify when screens extend beyond the scroll line.
- U1.07 App design should provide clear indications that elements are actionable. Interactive elements can be differentiated from non-selectable content through design choices that should be used consistently throughout the app (i.e., color, text style).
- U1.08 App design should support recognition over recall by keeping relevant information on screen rather than forcing users to remember it.
- U1.09 When possible, reduce the probability of data entry error by providing users with selectable options rather than requiring text entry.

- U1.10 Selectable items should be a minimum of 7 to 10 millimeters in length and width, with appropriate spacing allowance between items to avoid unintended selections.

Guideline U2 Readability

Text used within the app must be readable, understandable, and adjustable to accommodate ease of operation for a variety of devices, users and use environments. Text size adjustments should not alter the screen layout in a manner that could confuse users or prohibit ease of use.

Performance Requirements for Guideline U2

- U2.01 The default font size for paragraph text should follow the minimum standard guidelines for the platform of use (e.g., 17pt for iOS, 14sp for Android).
- U2.02 Different font sizes should be utilized to establish text hierarchy, with larger font sizes signifying headers and smaller font sizes used for paragraph text.
- U2.03 Apps should avoid presenting information in paragraph form when possible. When large amounts of information must be displayed, implement information chunking (i.e., intuitive grouping) or utilize lists and tables to facilitate learnability and memorability.
- U2.04 Text should incorporate appropriate spacing allowance between lines (e.g., 1.2 times the font height) to allow for breathability and readability.
- U2.05 Content should be written at reading level appropriate for the user population. Language for adult lay users without clinical knowledge should be written at or below a sixth-grade reading level.
- U2.06 Text should avoid use of jargon or acronyms that may not be familiar to users, particularly for lay users without clinical knowledge.

Guideline U3 App Navigation

Users should be able to navigate quickly and easily between screens to complete tasks. Navigation should meet user expectations, and should not dominate the interface or draw focus away from content.

Performance Requirements for Guideline U3

- U3.01 Users should be able to easily identify where they are in the app and how to navigate to different destinations. The navigational path should be logical, predictable, and easy to follow. For screens that users may need to access in succession, providing shortcuts may improve ease of navigation.
- U3.02 Minimize the number of taps, swipes, or screens required to navigate from one area of the app to another.
- U3.03 App design should facilitate reversible actions by allowing the user to navigate back to previous pages.
- U3.04 Menu options should be labeled intuitively such that users can easily locate information within the app. Users should not have to locate information by trial and error.

- U3.05 The app's main menu should be easily located and identified. Standard app design conventions would likely lead most users to look for a menu on the top, left-hand side of the screen. A collapsed menu is often associated with the three-bar "hamburger" icon that frequent app users are expected to be familiar with.

Guideline U4 Onboarding

Apps should facilitate an intuitive process for launching, registering, entering personal information (if applicable), and preparing for first-time use. As the users' first introduction to the app, a simple and intuitive onboarding process is critical in instilling user confidence that the app will provide a satisfying overall user experience.

Performance Requirements for Guideline U4

- U4.01 The app provides a launch screen that clearly identifies the name and purpose of the app, and gives the user intuitive options for initiating use.
- U4.02 Provide the user with opportunities either to access detailed instructions and product information or to bypass this and immediately begin app setup.
- U4.03 Users should be allowed to bypass entry of personal data if it is not critical for app functionality. Data that is needed for the app to work as intended (e.g., alert and notification parameters) should be mandatory to avoid inaccurate app behavior.
- U4.04 For apps with complex onboarding processes, entered data should be stored so that users can recover and avoid reentry if they are disconnected during the onboarding process.
- U4.05 When setup is complete, provide options for a walkthrough or tutorial on app use.
- U4.06 Apps should bypass onboarding for returning users, but allow users to update the data entered during onboarding at any time through intuitively named menu selections (e.g., Profile, Settings).

Guideline U5 App Feedback

Apps should provide sufficient feedback to inform the user of the results of their actions and promote understanding of what is going on in the system. Feedback includes how an app responds to user input, including providing messages to the user. Efficient and informative feedback ensures that users will be able to understand and perceive app actions without frustration. Guidelines associated with feedback related to notifications, alarms, and alerts can be found within Guideline U6.

Performance Requirements for Guideline U5

- U5.01 Feedback messages should appear in an expected and consistent location within the interface so that they are noticeable to the user (e.g., near the input location).
- U5.02 Feedback messages that are not urgent or associated with a safety risk should be unobtrusive to app operation.

- U5.03 Ongoing processes (e.g., loading) should utilize ongoing feedback to communicate status to the user. For longer processes such as downloading, inform the user of time remaining until the process is complete.
- U5.04 Feedback should occur quickly such that users can detect that their actions were successful. Avoid excessive lag between the action and the result (e.g., the user selects a menu option and the app takes several seconds to open the new page).
- U5.05 Error messages must, in clear and concise language understandable to the user, explain the problem and inform the user of the required corrective actions.
- U5.06 Users should be informed of data entry requirements. For example, if a user needs to choose a password during the setup process that requires both letters and numbers, this information should be stated at the point of data entry rather than only in the form of an error message.

Guideline U6 Notifications, Alerts & Alarms

Notifications (general reminders or updates to the user), alerts (non-urgent indicators intended to capture user attention), and alarms (urgent indicators that may be safety-critical) must consider both safety and usability to inform users when attention is required.

Performance Requirements for Guideline U6

- U6.01 Safety-critical alarms should utilize redundant signals to the user (e.g., visual, audible, tactile).
- U6.02 Users should be forced to acknowledge alarms before moving forward with other tasks.
- U6.03 Users should be given the choice to opt out of non-critical notifications and alerts.
- U6.04 Volume for audible notifications and vibration strength of tactile notifications should be customizable.
- U6.05 Notifications, alerts, and alarms should be stored as historical data so they are available for reference. This also provides a secondary resource for the user if a notification is dismissed in error. If an app allows the user to dismiss alerts and requires the user to select a reason for dismissal, this data should also be stored.

Guideline U7 Help Resources and Troubleshooting

Apps must incorporate help and troubleshooting features to guide the user when needed. Unavailable or unclear help features may lead to user confusion, frustration, and ultimately app abandonment.

Performance Requirements for Guideline U7

- U7.01 Apps should have an easy-to-locate help section that consolidates all information intended to assist the user.
- U7.02 Help features and informational links should be imbedded in the app when users may be likely to need them. Pop-ups are more appropriate for simple information such as terminology definitions, while links to the help section can be used for more complex troubleshooting.

- U7.03 Step-by-step walkthroughs should not be required for each completion of a task. Experienced users should be allowed to bypass detailed instructions.
- U7.04 Instructional information should avoid text-heavy paragraphs and give users easy-to-follow lists of task steps. For more complex processes, incorporate graphics or videos to supplement and/or replace text.

Guideline U8 Historical Data

Apps that gather data should store historical data in a manner that is easy for users to access, read and understand.

Performance Requirements for Guideline U8

- U8.01 For large data repositories, historical data should be sortable and filterable. Data sets for clinical-use apps that contain historical data for multiple patients should clearly identify patient name or ID.
- U8.02 Users should be informed if apps have a limited amount of data storage. Notifications may be used if an app will delete data after a specified amount of time.
- U8.03 Historical data should be displayed in a manner intuitive to the user and customized depending on the type of data (e.g., chronological, alphabetical). For example, an app that collects daily data from a user might present historical data in reverse chronological order so that a user has easy access to the most recent data collected.

Guideline U9 Accessibility

Apps should be designed and built to accommodate a wide variety of users, including those with individual differences such as perceptual impairment (visual or auditory), cognitive impairment and learning disabilities, and motor impairment. Apps designed to be adaptable will facilitate ease of use for all users, rather than just those with disabilities. Additionally, apps should aim to accommodate use with common assistive technologies (e.g., screen readers).

Performance Requirements for Guideline U9

- U9.01 App content should be adaptable and accessible for a variety of users. For example, provide text alternatives for multimedia (e.g., descriptions of images) or captions for video content and other alternatives. Content should be tailored such that it is presentable in either an audio or visual format without losing meaning.
- U9.02 Content layout should consider screen reader accessibility. This includes providing screen reader accessible alt text for images, and labels for buttons, icons, and loading states.
- U9.03 Apps should aim to accommodate a variety of input modalities, including gestures or use of an external keyboard. The content should not limit the user’s interaction to any specific input unless it is essential or to ensure security of content.
- U9.04 To the extent possible, app design should facilitate one-handed use.
- U9.05 Alternative input modalities, such as speech recognition, gestures, and handwriting recognition, may produce results that are less “exact” than standard input methods. These input modalities should require the user

to validate inputs (e.g., through use of confirmation screens or providing undo/redo options) so that unwanted actions are avoided.

- U9.06 Display of information and color choice should consider the most common visual impairments. For example, avoid using red and green in close proximity to accommodate users with red-green colorblindness.
- U9.07 Content should retain functionality and readability when adjustments are made to accommodate accessibility.

Guideline U10 On-Going App Evaluation

Throughout the entire development lifecycle, apps should undergo robust, iterative evaluations that follow a user-centered design process. Understanding the user perspective and evaluating technology to test assumptions is critical in developing safe and usable products, and apps that do not meet user expectations or are cumbersome to use are unlikely to be adopted. Apps requiring review by the Food and Drug Administration (FDA) should undergo testing evaluation that follows the FDA's guidelines for applying human factors and usability engineering to medical device design.

Performance Requirements for Guideline U10

- U10.01 Research on the target user population and anticipated use environments should be conducted to gather data on the characteristics of the app end users, whether clinical or laypeople, and assess how the environmental characteristics (e.g., noise, lighting, distractions) may impact safety and usability. This can be accomplished through activities such as ethnographic research, user interviews, and focus groups.
- U10.02 The target user population should be well-defined before initiating additional user activities (e.g., interviews, user testing). Evaluations should focus primarily on gathering data from those who fit the characteristics of expected user populations. This helps to ensure that the relevant physical attributes, perceptual cognitive expectations, and specific experiences of the end users are accounted for in design.
- U10.03 Apps intended to be used in a clinical environment should incorporate design elements that consider how the app may realistically fit into clinical workflow. Workflow assumptions should be reevaluated regularly to accommodate changes in current practices.
- U10.04 Apps should be designed to meet known usability heuristics. Trained human factors or usability specialists should be engaged to conduct heuristic evaluations using validated heuristic sets as part of usability assessment during the development process.
- U10.05 Apps should utilize tools such as failure modes and effects analysis or fault tree analysis to determine what if there are user tasks that could present risk to the patient or user. Apps should be designed to reduce or eliminate risk.
- U10.06 User testing should be conducted iteratively with the target end users of the app. User tests should produce both quantitative data on performance of app tasks, as well as qualitative feedback from study participants. Data gathered in the formative stages should be used to generate design updates that are expected to improve safety and usability.

- U10.07 A final summative (validation) test should be conducted to ensure the app can be used safely and successfully. The summative test should evaluate the major usage scenarios that a user is expected to encounter, and include evaluation of any user tasks that could have safety implications. A minimum of 15 users per distinct user group should complete the summative test to detect 90% of potential usability challenges.

References

https://www.nngroup.com/articles/usability-101-introduction-to-usability/

ISO 9241-11:2018 Ergonomics Of Human-System Interaction - Part 11: Usability: Definitions And Concepts

Web Content Accessibility Guidelines (WCAG) https://www.w3.org/WAI/standards-guidelines/wcag/

Faulkner L. Beyond the five-user assumption: benefits of increased sample sizes in usability testing. Behav Res Methods, Instruments, Comput. 2003;35(3):379–383.

Andriod's Material Design Guidelines (https://material.io/)

Apple's Human Interface Guidelines (https://developer.apple.com/design/human-interface-guidelines/)

Weiss BD. Health literacy: A manual for clinicians. Chicago, IL: American Medical Association Foundation and American Medical Association; 2003.

Multimodality in Mobile Computing and Mobile Devices: Methods for Adaptable Usability, Chapter: Designing Mobile Multimodal Applications, Publisher: IGI Global, Editors: Stan Kurkovsky, pp.106-135

Joehl, S. (2012, June 29). THE MOBILE ACCESSIBILITY LANDSCAPE. Retrieved from https://www.levelaccess.com

Jordan, J. B., & Vanderheiden, G. C. (2013). Modality-Independent Interaction Framework for Cross-Disability Accessibility. In P. L. P. Rau (Ed.), Cross-Cultural Design. Methods, Practice, and Case Studies (pp. 218–227). Part I, LNCS 8023. Springer-Verlag: Berlin Heidelberg.

App Operability (OP) Guideline

Operability will assess whether a mobile health app installs, loads, and runs in a manner that provides a reasonable user experience on mobile and web platforms.

Guideline OP1 On-Boarding

The app installs, launches, and runs consistently on the target device(s) and target operating system(s) for that app.

Requirements for Guideline OP1

- OP1.01 The app downloads and installs on the target device(s) and target operating system(s) as confirmed by user notification.
- OP1.02 The app launches and runs on the target device(s) that it is installed upon and, if it does not, the user is notified of the potential problem (e.g., to restart the app, Bluetooth, OS, etc.).
- OP1.03 The app runs on a defined & current version of the intended OS. The app documentation must state clearly what versions are supported. (e.g. Android versions).
- OP1.04 If the app requires that it be connected to a network, the app can connect and operates on the intended domestic and global carriers, Local Area Network (LAN) and Personal Area Network (PAN) and informs the user that the app is connected to a network and which network they are connected.
- OP1.05 The app functions as intended when not connected to a network. The user shall be informed of any differences between the apps functioning when connected or not connected to a network.

Guideline OP2 Connectivity

If applicable, the app connects consistently to any and all peripheral or accessory devices (e.g., NFC, Bluetooth, Continua), third party mobile application or software, regulated or unregulated, required for operation and/or marketed for use in conjunction with such app.

Requirements for Guideline OP2

- OP2.01 The app connects to the peripheral device(s) and operates consistently.
- OP2.02 The app has a mechanism to notify the user if the app fails to connect to any and all peripheral or accessory devices. The app needs to notify when data has been collected and not transmitted, if required.
- OP2.03 The app connects consistently to all third party mobile applications, software, and online user accounts, but such connection shall only occur after: (i) notifying user; (ii) requesting permission; and (iii) receiving consent from the user.
- OP2.04 The app has a mechanism to notify user of all updates applicable or necessary for the app to connect to any such device, application, software or online user accounts.

Guideline OP3 Access to App Publisher

A method for contacting the app publisher and technical support is provided.

Requirements for Guideline OP3

- OP3.01 The app publisher's contact information—including but not limited to, mailing address, email address, or other clearly identified method (e.g. IM, Skype) for support and general inquiries, web address and/or DNS address—is provided within the app, or the app provides a link to a webpage that contains the same information.
- OP3.02 The app provides a method for users to submit feedback to the app publisher for purposes of improving the user experience, including without limitation, any technical issues, bugs, and errors detected by users.

Guideline OP4 Documenting & Detailing Releases

The app publisher shall document the feature detail and include a historical view of prior releases.

Requirements for Guideline OP4

- OP4.01 The app should have a history of updates including details of changes over time.

Guideline OP5 Operability with EHR

Electronic Health Record (EHR) systems optimized for mobile devices or apps for certified EHRs (EHRs that have been certified by a Federally-designated Authorized Testing and Certification Body) maintain secure and operable data exchange. Certified EHRs may consist of complete EHRs or EHR modules.

Requirements for Guideline OP5

- OP5.01 The app operates in accordance with the documented functionality provided by the Certified EHR.
- OP5.02 Documentation is provided regarding any relevant EHR certification received.
- OP5.03 The EHR systems with which the app connects are specifically enumerated and documentation of the interoperability with each specified EHR is provided.
- OP5.04 The details and description of the data fields that the app saves, sends to, and/or receives from each specified EHR system regarding patient information is provided.
- OP5.05 The app maintains (at rest) and transmits (in motion) patient information in a secure, HIPAA-compliant manner, as applicable (see Guidelines S2, S3, and S4).

Guideline OP6 Connectivity with PHR

An app that is intended to connect to a Personal Health Record (PHR) enables users to send and retrieve patient information between a mobile device and the PHR and does so in a secure manner.

Requirements for Guideline OP6

- OP6.01 The PHR systems with which the app connects (e.g. Microsoft HealthVault, Blue Button etc.) are specifically enumerated and documentation of the interoperability with each specified PHR is provided.
- OP6.02 The details and description of the data fields that the app saves, sends to, and/or receives from each specified PHR system regarding patient information (e.g., medical history, diagnoses, treatment plan, medications, laboratory results, radiology images, etc.) is provided.

Guideline OP7 Medical Device Status

If applicable, the app publisher certifies that it is not a medical device, or certifies that the app constitutes a medical device as defined by the U.S. Food and Drug Administration (FDA), has ascertained its correct classification, and either certifies that the app complies with all applicable FDA regulatory requirements.

Requirements for Guideline OP7

- OP7.01 The app publisher has ascertained that the app, including any and all peripheral devices required or intended for operation and/or marketed for use in conjunction with such peripheral devices, is an MDDS, Class I, II or III medical device.
- OP7.02 The app publisher provides documentation demonstrating that the app complies with all applicable FDA requirements, including but not limited to: Establishment registration; Medical Device Listing; Premarket Notification 510(k), unless exempt, or Premarket Approval (PMA); Investigational Device Exemption (IDE) for clinical studies; Quality System (QS) regulation; Labeling requirements; and Medical Device Reporting (MDR).
- OP7.03 The app publisher has a mechanism to immediately notify all users about an FDA-approved app that is recalled, the subject of an FDA advisory, or similar status that calls the app's safety and/or effectiveness into question.
- OP7.04 If the app does not constitute a medical device as defined by the FDA, the App publisher certifies that the app is not a medical device by written attestation on the Alliance Submission Form.

Appendix 1

Acronyms

Many acronyms are used in this document. The following table provides the full term for each acronym.

Acronym	Full Term
AAMC	Association of American Medical Colleges
BA	Business Associate refers to a person/entity that requires disclosure of ePHI in order to deliver their product/service to or on behalf of a Covered Entity.
BAA	Business Associate Agreement (required in certain circumstances under HIPAA and HITECH [defined below])
BT	Bluetooth standard as defined by IEEE 802.15 and BT SIG (Bluetooth Special Interest Group)
CDMA2000	Refers to a family of 3G standards providing high-quality voice and broadband data services over wireless networks
CDS	Clinical Decision Support software
DNS	Domain Name System
EHR	Electronic Health Record (also referred to as EMR – Electronic Medical Record)
FCC	Federal Communications Commission
FDA	U.S. Food and Drug Administration
FTC	Federal Trade Commission
GPS	Global Positioning System (a satellite-based navigation system)
GSM	Global System for Mobile Communications (originally, Groupe Spécial Mobile)
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
LAN	Local Area Network
MMS	Multimedia Messaging Service
NFC	Near Field Communication
PHI	Protected Health Information
PSTN	Public Switched Telephone Network
SMS	Short Message Service
URI	Uniform Resource Identifier
W3C	World Wide Web Consortium

Appendix 2

Guidelines for Mobile Health App Content Assessment for Xcertia Standards

CONDITION	ORGANIZATION	GUIDELINE URL	UPDATE STATUS OR ALERTS

Hyperlipidemia	NHLBI / ATP	http://www.nhlbi.nih.gov/guidelines/cholesterol/atp3_rpt.htm & http://www.nhlbi.nih.gov/guidelines/cholesterol/atp3upd04.htm	http://www.nhlbi.nih.gov/guidelines/indevelop.htm#status
Hypertension	NHLBI / JNC	http://www.nhlbi.nih.gov/guidelines/hypertension/jnc7full.htm	http://www.nhlbi.nih.gov/guidelines/indevelop.htm#status
	AHA / ACC / ASH	http://circ.ahajournals.org/content/131/19/e435	
Cardiovascular?	AHA		(Simple 7 program for wellness) see their weight loss guidelines as well
Stroke	ASA	Stroke/ CVA AHA http://my.americanheart.org/professional/StatementsGuidelines/ByTopic/TopicsQ-Z/Stroke-Statements-Guidelines_UCM_320600_Article.jsp	Added May 2015
Osteoarthritis	ACR	https://www.rheumatology.org/Practice/Clinical/Guidelines/Osteoarthritis_(Members__Only)/	
	AAFP	http://www.aafp.org/afp/2012/0101/p49.html	
Rheumatoid Arthritis	ACR	https://www.rheumatology.org/Practice/Clinical/Guidelines/Rheumatoid_Arthritis_(Members__Only)/	
	AAFP	http://www.aafp.org/afp/2012/0101/p49.html	
Migraines	AAFP / ACP-ASIM	http://www.aafp.org/afp/2003/0315/p1392.html	
	AAN	http://www.neurology.org/content/55/6/754.full	
Chronic Pain	AAPM	http://www.painmed.org/library/clinical-guidelines/	
Diabetes	ADA	http://professional.diabetes.org/ResourcesForProfessionals.aspx?cid=84160	January *Diabetes Care* supplement
Osteoporosis	NOF	http://www.nof.org/files/nof/public/content/file/950/upload/523.pdf	
Constipation	WGO	http://www.worldgastroenterology.org/assets/downloads/en/pdf/guidelines/05_constipation.pdf	
	ACG	http://gi.org/acg-institute/evidence-based-reviews/	

Anxiety	APA	http://psychiatryonline.org/guidelines	
Depression	APA	http://psychiatryonline.org/guidelines	
Crohn’s Disease	ACG	http://gi.org/guideline/management-of-crohn%E2%80%99s-disease-in-adults/	
GERD	ACG	http://gi.org/guideline/diagnosis-and-managemen-of-gastroesophageal-reflux-disease/	
Ulcerative Colitis	ACG	http://gi.org/guideline/ulcerative-colitis-in-adults/	
IBS	ACG	http://www.nature.com/ajg/journal/v109/n1s/full/ajg2014187a.html	
Pregnancy	ACOG	Practice Bulletin: http://www.ncbi.nlm.nih.gov/pubmed/?term=ACOG%20Committee%20on%20Practice%20Bulletins-Gynecology%5BCorporate%20Author%5D	
Gestational Diabetes	ACOG	http://www.acog.org/Womens-Health/Gestational-Diabetes	
Infertility	ACOG	Practice Bulletin: http://www.ncbi.nlm.nih.gov/pubmed/?term=ACOG%20Committee%20on%20Practice%20Bulletins-Gynecology%5BCorporate%20Author%5D	
Overactive Bladder/ Urinary Incontinence	AUA	https://www.auanet.org/education/guidelines/incontinence.cfm (surgical)	
	ACP	http://annals.org/article.aspx?articleid=1905131 (nonsurgical)	
Asthma	NHLBI	http://www.nhlbi.nih.gov/guidelines/asthma/asthsumm.pdf	
COPD	GOLD	http://www.goldcopd.org	
Breast Cancer	ASCO	http://www.asco.org/search/site	
	NCCN	http://www.nccn.org/professionals/physician_gls/f_guidelines.asp#site	
Prostate Cancer	ASCO	http://www.asco.org/search/site	
	NCCN	http://www.nccn.org/professionals/physician_gls/f_guidelines.asp#site	
Colorectal Cancer	ASCO	http://www.asco.org/search/site	
	NCCN	http://www.nccn.org/professionals/physician_gls/f_guidelines.asp#site	

Acromegaly	AACE	https://www.aace.com/files/acromegaly-guidelines.pdf	
Hyperparathyroidism	AACE / AAES	https://www.aace.com/files/position-statements/hyperparathyroidps.pdf	
Epilepsy	AAN	https://www.aan.com/Guidelines/home/ByTopic?topicId=23	
Fibromyalgia	ACR	https://www.rheumatology.org/Practice/Clinical/Patients/Diseases_And_Conditions/Fibromyalgia/	
Benign Prostatic Hyperplasia	AUA	https://www.auanet.org/education/guidelines/benign-prostatic-hyperplasia.cfm	
Nephrolithiasis	AUA	https://www.auanet.org/education/guidelines/management-kidney-stones.cfm	
Drug reference	PDR	http://www.pdr.net	