233 N. Michigan Ave.,21st Fl.
Chicago, IL 60601-5800

phone » (312) 233-1100
fax » (312) 233-1090
web » www.ahima.org

American Health Information Management Association®

AHIMA Comments on Xcertia™ mHealth App Guidelines

May 15, 2019

The following comments are submitted on behalf of AHIMA's Chief Executive Officer, Wylecia Wiggs Harris, PhD, CAE

Committed to the mission of empowering people to impact health, the American Health Information Management Association (AHIMA) supports the overarching goal of Xcertia's™ mHealth App guidelines. Increasingly, there is a pressing need to develop a framework to evaluate the trustworthiness and transparency of existing and new mobile health applications to help foster consumer and physician confidence in the use of these apps. We offer the following comments in response to the updated 2019 Xcertia™ App Guidelines.

In general, we recommend that Xcertia™ consider including as part of the guidelines a section on "definitions." There are a number of terms within the guidelines that appear to have the same or similar meaning; however, the guidelines lack the context to determine whether there is a distinction between them. For example, the guidelines use such terms as "app publisher," "app designer," "app owner," and "app developer"—are these intended to have the same meaning, or do they represent different sets of actors? We also recommend defining "user" within the guidelines. While it can be inferred by reading the guidelines that the user could be clinicians and/or consumers, we believe there is value in clarifying that a user under the guidelines could include both populations. Furthermore, we believe there is merit to including in the proposed section of "definitions," terms that are already in statute and/or regulation such as Protected Health Information (PHI), Personally Identifiable Information (PII), and Business Associate Agreement (BAA) as some app developers may not be as familiar with such terminologies.

App Privacy (P) Guidelines

AHIMA recommends that Xcertia™ clarify whether "personal information" is intended to be used as a term of art in the guidelines. For example, Black's Law Dictionary defines personal information as, "any part of information that is recorded about an individual person. Includes the name, email, address, ethnicity, race, identifying number, employment history, etc."[1] In contrast, California's Consumer Privacy Act (CCPA) defines "personal information" as:

> Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:
>
> (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number or other similar identifiers

[1] Available at: https://thelawdictionary.org/personal-information/.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80
(C) Characteristics of protected classifications under California or federal law
(D) Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
(E) Biometric information
(F) Internet or other electronic network activity information, including but not limited to browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement
(G) Geolocation data
(H) Audio, electronic, visual, thermal, olfactory, or similar information
(I) Professional or employment-related information
(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 USC §1232g, 34 CFR Part 99)
(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.[2]

Given the variance in how "personal information" is defined in these two instances, we recommend that Xcertia™ clarify how the term "personal information" is intended to be construed under the guidelines. Such a clarification will help ensure that app developers and users have a clear understanding of what personal information should be protected by the app developer in accordance with the guidelines.

Guideline P1 – Notice of Use and Disclosure

AHIMA recommends that the Privacy Notice describe how the organization "collects, uses, retains *and deletes* their data." P1.13 appears to address the deletion and/or destruction of all personal data should a user decide to cancel or delete their account, however, for clarity and consistency purposes, we recommend this be made clear in the preamble of Guideline P1.

We also recommend that the Privacy Notice be written in plain language to enable users to gain an enhanced understanding of how the organization collects, uses, retains and deletes their data. We recognize that the accessibility of the Privacy Notice is covered under Guideline P6—General Data Protection Regulation (GDPR) but we recommend requiring that the Notice be in plain language, transparent, and accessible under both guidelines.

Requirements for Guideline P1

P1.05 AHIMA recommends the P1.05 requirement include, ". . . all third parties such as in-app advertisers *and third-party analytics services*." Recent reports of apps using Facebook software to create and send custom app events that include sensitive data without the user's consent which are in turn used by developers to target their users with ads raises significant privacy concerns.[3] Furthermore, we recommend that a user should have the option to opt-out of passing data on to third-party analytics

[2] CA Civ. Code §1798.140(o)(1).
[3] "You Give Apps Sensitive Personal Information. Then They Tell Facebook" *Wall Street Journal* (February 22, 2019).

services when such software will be used by the app developer to target the user with ads on third-party platforms such as Facebook, Instagram, Google, etc.

P1.09 AHIMA supports the requirement that the Privacy Policy inform users of how they can obtain a copy of their personal information that was collected by the app, including 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, in compliance with the HIPAA Privacy Rule, and any other state or international laws, rules or regulations. Often, consumers are not aware that they have no legal right to nor control of data collected by an app and that it is often left to the discretion of the app developer as to whether a user's PHI or PII may be shared with the individual. Allowing users to obtain a copy of their personal information as well as the ability to correct and update the information supplied will not only preserve an individual's right to access their health information as granted under HIPAA but provide greater uniformity in how a user may access their protected health information and/or personal information no matter where it travels.

P1.12 It is unclear here whether an app publisher must meet all of the requirements under P1.12 to be able to share personal data with a third party. We recommend that Xcertia™ provide greater clarity as to what requirements must be met under P1.12.

P1.14 The requirement that a mechanism be in place to notify users of changes to the Privacy Policy appears duplicative of P1.03 where an owner represents that commercially reasonable efforts are used to notify users of any material changes to its Privacy Policy. We recommend P1.14 be eliminated from the guidelines.

P1.16 AHIMA supports the intent of P1.16 to promptly notify users in the event of a breach and in accordance with applicable state, federal and country laws. However, we recommend that Xcertia™ clarify whether the most rigorous breach notification requirements would apply in circumstances where federal, state and/or international jurisdictions conflict.

We appreciate the opportunity to provide comments on Xcertia's™ revised 2019 mHealth App Guidelines and we look forward to collaborating with Xcertia™ and its partners to further develop and disseminate the guidelines. Should you have any questions regarding our comments, please contact Lauren Riplinger, Senior Director, Federal Relations, at lauren.riplinger@ahima.org and (202) 839-1218.