Emory Mobile App Review and Distribution Process for Public App Marketplaces

Status of this Document

This is the current description of the Emory Mobile Application Review Process for apps bound for general availability releases in public app marketplaces. If your application is presently only intended for internal Emory distribution, please see the page entitled Emory Mobile App Review and Submission Process for Internal Emory Distribution. This document describes the process in use and not an ideal process. Comments and suggestions are welcomed as comments on this page, or you may send feedback to Steve Wheat at <swheat@emory.edu>.

Step 1: Request Internal and Public Distribution of the Application

Mobile apps must first be distributed to the internal Emory reviewers using the Emory Mobile App Catalog, a type of internal Emory app store. App owners should complete the Internal Mobile App Distribution Request Form to start this process. These requests are generally completed within two or three days. A mobile app can usually be distributed internally to a restricted group in two or three days from the time of the request. Distribution to a large internal audience usually take two to three weeks to complete the internal review process, and distribution on public marketplaces may take several weeks to several months depending on the complexity of the app and the compliance and commercial implications of the app. Once the app has been posted to the internal app catalog, the mobile app review coordinator will reach out to you with more details regarding the review process. At this point, please complete the Public Mobile App Distribution Request.

Step 2: Office of Technology Transfer Intellectual Property Analysis

Emory units desiring to release mobile applications should contact the Emory Office of Technology Transfer (OTT) for a review of the intellectual property and commercial prospects of the application. This process includes completion of an intellectual property (IP) disclosure. In general, any application owned by Emory will be released under the Emory brand and through the Emory App Store or Marketplace accounts. There may be exceptions to this general rule in the case of collaborations between Emory and other partners or in a case where technology has been licensed to a third party.

Rajsekhar Guddneppanavar (rguddne@emory.edu) is the primary contact with OTT.

Step 3: Communications & Public Affairs Branding Review

Following the intellectual property analysis in Step 2, mobile applications that are to be released under the Emory brand undergo a branding review with Communications & Public Affairs. Communications & Public Affairs has prepared a set of written guidelines and resources for the proper branding of Emory mobile applications. Unless a compelling business reason be can provided as to why a public mobile application should not carry Emory visual identity, branding guidelines should be followed. Stanis Kodman (stanis.kodman@emory.edu) is the point of contact with Communications & Public Affairs for Emory University. Mark Swilley (mark.swilley@emoryhealthcare.org) is the point of contact with Emory Healthcare Marketing.

Step 4: Legal Counsel Review

OTT will inform and consult with Emory Legal Counsel on the outcome of the IP review in step 2 and any specific plans for commercializing or charging for the mobile applications, its terms of use, etc.

Step 5: Compliance and Regulatory Review

Emory University and Emory Healthcare compliance officers review the mobile application to determine whether or not Emory's HIPAA compliance or other appropriate compliance policies apply. Emory's compliance officers provide the following general guidance in determining whether or not HIPAA applies to a mobile application:

1. If the mobile application collects, stores, or transmits personal health information for the personal use of the consumer and not for Emory people in their role as researcher, clinician, or support role, then HIPAA does not apply to the application.
2. Add item about FDA regulations and review [Kris West to suggest text].
3. If such an application provides Emory clinicians access to the personal health information for the purposes of billable patient care, then HIPAA does apply to the application.
4. If such an application provides researchers access to personal health information for the purposes of research or non-billable patient care, then HIPAA does not apply to the application, but Emory's security policies and practices for applications that handle personal health information still apply. See item #5.
5. All such applications that collect, store, or transmit personal health information must implement appropriate information security measures to protect personal health information, regardless of whether or not Emory's HIPAA compliance policies apply.
6. Emory Information Security has compiled a list of mobile app defaults and mobile app specific security review questions that must be considered when designing, developing, and distributing mobile apps.

Step 6: Technical & Information Security Reviews

Using the answers to the mobile app security questions, Emory Library and Information Technology (LITS) Security performs a high-level technical review of the application to determine if there is a need for any further detailed security and compliance reviews of the application. For example, if the application collects and stores ePHI, credit card information, or other compliance related data, Emory OIT will inform the owners of the application of relevant policies and any practices required by those policies. Additional materials may be required, depending on the type of review specified. The organizer of the technical review team will contact application developers and help them prepare any additional materials.

If an in-depth security review is required, a meeting is scheduled with representatives of Emory Information Security to walk through a mobile app security checklist based on the security, compliance, and regulatory requirements that are relevant to the particular application.

Step 7: Library and Information Technology App Store Posting Review

Based on the outcome of the preceding reviews, remediations to the app may be requested by individual approving groups. Once all reviews have been completed and approvals gathered, Emory LITS will copy the appropriate marketplace submission templates for the application. There are two submission templates: one for the Apple App Store and one for Google Play. Each submission template has the list of relevant artifacts that must be assembled to submit an application to each marketplace. Application owners will complete these templates and append all images and files to the template. Once the template is complete, LITS staff will submit the application with the appropriate marketplaces.

The following are links to the Marketplace Submission Templates:

- Apple App Store Submission - Template
- Google Play Store Submission - Template

Subsequent App Update Submissions

For subsequent application updates, application owners should update the technical review template and if there are substantial changes, request another review. For example, if the nature of the data being collected or stored by the application has changed and now ePHI is being collected when it was not before, then a new review should be scheduled. Application owners should also update the marketplace submission forms relevant to their applications for each subsequent submission.

Public App Review and Distribution Process Flow

Please click on the image below to enlarge.