Emory Review Process for Vendor- or Partner-provided ESB, Web, or FHIR Services

Status of this Document

This is the draft description of the Emory Review Process for consumption of vendor- or partner-provided ESB, Web, or FHIR services. This process proposal pertains to cases in which Emory applications which to consume services and events exposed by applications operated externally from Emory. This document describes a proposed process that is not presently in use. Comments and suggestions are welcomed as comments on this page or you may send feedback to Steve Wheat at <swheat@emory.edu>.

Process Goals

The goals of this process are to implement Emory's policy for vendor- or partner provided-ESB, web, and FHIR services by:

1. Obtaining and recording approval of appropriate external data custodians for release of data and logic
2. Implementing applicable compliance and security requirements
3. Tracking and recording services and their use in Emory's service registry and dashboard
4. Assessing additional risk of invoking services of providers on the internet
5. Implementing appropriate public service security, auditing, and countermeasures

Step 1: Request Proposed Use of a Vendor- or Partner-provided Service

In order to review a proposed use of an existing vendor- or partner-provided service, complete the Vendor- or Partner-provided Service Review Request Form to start the process. The appropriate LITS integration team for University or Healthcare IT will receive the request to coordinate the review of the requested service use, enter the service into the Emory ESB/Web Service Dashboard, initiate the review, and make contact with the requestor to start the review and prepare to implement the request if approved.

Note that neither LITS nor the requesting client should begin invoking the external service for a new use without completing this process. For many projects there is a desire to invoke services in a development, test, and/or demo environment to facilitate proofs-of-concept or demos with vendors or public apps. This too may only be done with certification from the data custodian in Step 2 that no sensitive data or processes can possibly be exposed in these non-production environments. Once this certification is obtained in step 2, non-production activities with non-sensitive data and logic may process.

Step 2: Data Custodian Review

Note that in this case there may be both Emory and external data custodians involved. Emory may need to obtain and record approvals from both Emory and vendor- or partner- data custodians or confirm that contracts with external entities adequately constitute such approval. LITS identifies the data custodian(s) for the data the ESB, web, or FHIR service exposes from the Emory ESB/Web Service Dashboard and forwards the request to the data custodian for approval. Data custodians are determined by the business owners of the data as part of the SOA governance process. LITS identifies the specified owners by using the dashboard list. If upon review by the data custodian it is unclear whether the request should be approved or denied, a meeting of the SOA governance team (all reviewers in this process) may be called by the data custodian or the requestor to discuss the request.

Step 3: 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. If such an application provides Emory researchers or clinicians access to the personal health information for the purposes of research or patient care, then HIPAA does apply to the application.
3. 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.

4. [Note: Brad Sanford and Steve Wheat should draft a list of the common security measures that apply to all such mobile applications and another list of the additional measures that would typically apply for applications subject to HIPAA compliance policies, so mobile app designers can plan for these measures in advance]

Step 4: Technical & Information Security Reviews

Emory Library and Information Technology (LITS) performs a high-level technical review of the application to determine if there is a need for any 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 IT will inform the sponsors of the application of relevant policies and any practices required by those policies. See the template for this cursory review. Once this cursory template is completed a technical review will be scheduled by Emory University or Emory Healthcare technical review team, depending on whether the application is considered and Emory University or Emory Healthcare application. 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 a 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.

Note that all consumption of publicly exposed ESB, Web, and FHIR services are potentially subject to additional security and auditing measures beyond internally distributed services. Projects should allow additional time for the implementation of any additional measures specified in the review of a publicly-exposed ESB, web, or FHIR service.

Subsequent App Update Submissions

For subsequent application updates, application users should update the desired uses for the app and supporting information. 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 internal submission forms relevant to their applications for each subsequent submission.

As a first step, we are cataloging all vended mobile apps endorsed or recommended by LITS and entering them into the mobile app catalog. The form below is intended to help collect information on these applications. For more information on mobile app distribution see the Mobile Application Review and Distribution Processes page.