# Integration Platform as a Service Feasiblity Study Project

## Background

With the advent of integration platform as a service offerings (PaaS) it may be possible to move our existing integration service to cloud deployment and focus more on administering integrations rather than the middleware that runs these integrations. The limiting factor to date has been security and performance concerns. However, top-tier research and health science center UC San Francisco has recently used MuleSoft CloudHub to build HIPAA complaint integration services. We know it is possible to run our existing OpenEAI integration services within this type of infrastructure, so a feasibility and cost assessment of migration to this platform is desired.

## Goals

Complete a preliminary security review, HIPAA business associate agreement, and initiate a limited trial service. Document a pattern for running Emory's existing service in CloudHub. Execute a representative migration of sufficient size to estimate the cost and effort to migrate and operate on this platform. Prepare a summary report.

## Project Phases

1. Preliminary security review (April, May)
2. BAA and service agreement (June-September)
3. Document migration patterns (October, November)
4. Evaluate migration strategies (November, December)
5. Implement representative migration (Jauary, February)
6. Testing and benchmarking (February, March)
7. Final estimation and summary report (April, May)
8. Present results (June)
9. Follow-up tests, assessment, report updates (July)

This project is presently pending initiation anticipated to complete in August 2015.

## Issues

Presently progress is pending the execution of a business associate agreement (BAA) and a service agreement. Our most recent communication with the vendor outlined the following:

Business issues that need to be resolved before POC:

1. Mulesoft must sign Emory’s BAA
2. Mulesoft must have appropriate BAAs with any downstream service providers as required by HIPAA (including HITECH and the omnibus final rule)

Security issues that need to be resolved as part of a POC:

1. Validate Mulesoft’s compliance status with PCI, HIPAA and HiTrust (completion target was 3rd Quarter)
2. Complete Emory’s HIPAA risk assessment process
3. Determine how to mitigate identified risks
4. Reevaluate status of Mulesoft monitoring and response capabilities (per Mulesoft this is a work in progress)
5. Determine how to monitor Emory developed Apps within Mulesoft environment (which Mulesoft does not monitor at all)
6. Specifically determine how we can get access to Mule application logs, preferably streamed in realtime.
7. Determine if the logs can be fed into SIEM (and if they have any value)
8. Determine if the logs are sufficient for our development and security needs
9. Limit VPC to only Emory IP address ranges
10. Document network controls that are unavailable in AWS environment
11. Identify any compensating controls to minimize this risk / manage the risk to an acceptable level
12. Determine how to implement requirements in section 5 of ASP requirements document in the Mule workers we control

## Documentation

1. CloudHub Feasibility Assessment wiki page (forthcoming)
2. UCSF CareWeb case study