Migrate an Application to Project Hosts' HIPAA/HITRUST Compliant Security Envelope in Azure

Introduction

While many factors must be carefully considered before deciding which on-premises applications should be moved to the cloud for economic or other reasons, there are some general guidelines that we typically encounter in working with healthcare providers. Cloud migration should be considered under the following circumstances:

- Applications that are not **ISO 27001, HIPAA** or **HITRUST** compliant, yet need to be
- Customer-facing **web-or-mobile applications** that are operational or in-development
- Applications and OS/database platforms that are **several revisions back** which are scheduled for larger scale upgrades (such as Windows Server/SQL Server or Linux/MY SQL)
- Any on-premises infrastructure that is: **limiting** application performance, cannot scale up or down as needed, lacks adequate storage, or cannot meet disaster recovery or business continuity needs
- Any on-premises application / solution which requires additional **integration** with external PHI / EHR systems in a secure manner (i.e. hybrid-cloud solutions)
- Workloads that can be more efficiently and economically managed in a cloud platform

HIPAA/HITRUST Security Envelope

Project Hosts has created an environment on Microsoft Azure that has been audited and certified to be compliant with both HIPAA and HITRUST security standards. Project Hosts has the ability to bring customer applications into this "Security Envelope" as long as they are compatible its security architecture. Namely, applications must be

- Able to run on one of two OS/DB platforms: Windows Server/MS SQL (2012 R2 or higher) or Linux/MySQL
- Compatible with having a Sophos anti-malware and an Azure OMS logging client installed on each server
- Able to be authenticated by Active Directory or SSO if single sign-on is desired
- Accessible to users via either HTTPS or a virtual desktop

Applications of this type may be migrated into the HIPAA/HITRUST Security Envelope where they are protected by all of the security protections, policies and procedures in place required for HIPAA and HITRUST.

Application Migration POC

Project Hosts engineers will work with your IT team to migrate your Application into the Security Envelope.

- Provision 2 dedicated servers (ES2's) in 2 dedicated Azure subnets protected by Azure NSG access controls
- Install your application and database or virtual desktops on those servers
- Restore database backups from your on-premise environment into the cloud environment
- Run a vulnerability scan and discuss how remediation could be done if ongoing services were procured
- Ensure your users are able to access the application (up to 10 users for POC pricing)
- Provide the other Security Envelope services listed below for 30 days while you test the environment

Ongoing pricing for continuing to have your Application deployed in Project Hosts' HIPAA/HITRUST Security Envelope can be quoted based on Application resource requirements.

PROJECT HOSTS' HIPAA/HITRUST SECURITY ENVELOPE SERVICES

Applications in Project Hosts' HIPAA/HITRUST Security Envelope benefit from the following services:

I. Performance Management
II. Security Management
III. Access & Application Management

IV. HIPAA/HITRUST Compliance Management

All three service offerings are required in order to implement the full set of HIPAA/HITRUST controls for an environment.

I. PERFORMANCE MANAGEMENT

Project Hosts' Performance Management services include the following:

- 24/7 performance monitoring and alerts
- Provisioning servers or scaling to larger or smaller servers
- Weekly virtual image backup and restore
- Weekly, daily, hourly database backup and restore
- Managing and testing DR restores in secondary Azure data center
- OS systems administration for Windows and Centos Linux
- Database administration for MS SQL and MySQL
- 24/7 technical support
- Performance optimization recommendations

II. SECURITY MANAGEMENT

Project Hosts' Security Management services include the following:

- Azure Web Application Firewall
- Azure subnets with their NSG "firewall" access controls
- Active Directory to manage servers, group policy, and user authentication
- Web Application Proxy (WAP) servers
- Centrally managed anti-malware and Host Intrusion Prevention
- System systems
- Remote Desktop Gateway servers for secure remote administration
- Logging configuration, collection, alerting, and review using Azure OMS
- OS and database scanning, patching and vulnerability tracking
- Project Hosts' Centralized inventory tracking and alerting system (Admin Center)
- Incident response system with periodic tests

III. ACCESS & APPLICATION MANAGEMENT

Project Hosts' Access Management services include the following:

- Single sign-on (SSO) from other authentication systems
- Quarterly web app vulnerability scanning - Monthly cloning of servers in the deployment for scanning (where scanning production servers would cause disruption)
- Coordination with customer to patch web applications or modify configurations
- 24/7 support of applications on Project Hosts' approved application list
- Project Hosts' user authorization and administration tool (PH Portal)

IV. HIPAA & HITRUST COMPLIANCE MANAGEMENT

Project Hosts' Compliance Management services include the following:

- Maintaining HIPAA and HITRUST policies and procedures along with evidence of their implementation
- Annual ISO 27001 third-party audits to verify continued compliance with both ISO and HIPAA standards
- Annual HITRUST third-party audits to verify continued compliance with the HITRUST standard