PROJECT HOSTS™
Security Compliant Clouds

HIPAA / HITRUST Compliant Azure Customer Subscription

Project Hosts provides two service offerings that together allow a customer to become fully HIPAA/HITRUST compliant for a deployment on Azure: Azure Managed Services, which includes Performance Management, Security Management, and Apps Management, and Documentation and Assessment Management for HIPAA, NIST 800-66 and HITRUST.

AZURE MANAGED SERVICES

Project Hosts provides three Azure Managed Services offerings:

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

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

I. AZURE PERFORMANCE MANAGEMENT

Project Hosts' Azure 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. AZURE SECURITY MANAGEMENT

Project Hosts' Azure Security Management services include implementing and managing the following:

- HIPAA Security Controls
- HITRUST Security Controls
- Azure subnets with their NSG "firewall" access controls
- An Active Directory Domain to manage servers and group policy
- Web Application Proxy (WAP) servers as the controlled front door to the Deployment
- McAfee Host Intrusion Prevention System (HIPS) on every server, and EndPoint Protection centrally managed by ePolicy Orchestrator
- Remote Desktop Gateway servers for secure remote administration
- Logging configuration, collection, alerting, and review
- OS, DB and application software patching
- Project Hosts' Centralized inventory tracking and alerting system (Admin Center)
- Incident response system with periodic tests

ABOUT PROJECT HOSTS

Established in 2003, Project Hosts is a cloud solutions provider (CSP) that specializes in securing, managing, and meeting regulatory security compliance standards for Windows and Linux solutions in Azure environments and ensuring compliance at the SaaS level for HIPAA, HITRUST, NIST 800-66, ISO 27001, FedRAMP, Moderate, High and DoD IL 4/5 security levels.

Our comprehensive set of Azure managed services extend compliance beyond the infrastructure (IaaS) and platform (PaaS) level to protect entire applications at the Software (SaaS) level, implementing controls related to access, authentication, encryption, auditing, scanning, business continuity, change management, incident response, privacy, annual assessment, penetration testing, and required documentation.

Healthcare organizations, federal, state, and local government agencies, and enterprises rely on us to ensure they have a cloud solution that meets their business needs, their budget, and most importantly, protects their business, employee, customer, and patient data from unauthorized access or theft.

Our core services, that include deploying, securing, managing and monitoring Applications and Workloads, can be performed in a Customer's Azure Subscription, licensed directly with Microsoft, or within a Project Hosts' Azure subscription.

Project Hosts - 333. W. El Camino Real #220, Sunnyvale, CA 94087 USA info@projecthosts.com www.projecthosts.com

III. AZURE ACCESS & APPLICATION MANAGEMENT

Project Hosts' Azure Access Management services include implementing and managing 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 DOCUMENTATION AND ASSESSMENT MANAGEMENT

With more than 13 years of expertise in securing Microsoft cloud solutions, the Project Hosts security team understands the exact control responses, technical implementations, and evidence that are required to demonstrate full SaaS compliance of HIPAA and HITRUST standards for an environment built on Microsoft Azure IaaS.

Neither HIPAA nor its amendment (HITECH) have official compliance certifications by their governing bodies. The way that most organizations demonstrate HIPAA compliance is to include HIPAA policies and evidence in annual third-party assessments of a related standard that does have an official certification. For example, Microsoft Azure includes HIPAA policies in their annual ISO 27001 audit, and AWS includes HIPAA policies in their annual FedRAMP (NIST 800-53) assessment. For the latter, NIST 800-66 provides guidance as to how to map HIPAA controls to NIST 800-53 controls.

HITRUST is an emerging standard for the healthcare industry that incorporates HIPAA requirements in a more prescriptive manner. Like ISO 27001 and FedRAMP, HITRUST certifies third-party auditors who can then confer an official certification of compliance to an organization. The resultant HITRUST certification is called CSF-Certified.

In addition to third-party certifications, both HIPAA and HITRUST have self-assessments that can be used to verify compliance with those standards.

If Project Hosts is providing the Azure Managed Services described above, then a customer may also elect to have Project Hosts provide the following services:

- Documentation of Security Controls, Policies, Procedures, and Implementation Proposals
- HIPAA and HITRUST self-assessment Support
- Third-party assessment Management or Support

V. DOCUMENTATION OF SECURITY CONTROLS

The HIPAA security rule has a set of controls that is mapped to NIST 800-53 by a set of controls in NIST 800-66. In addition, HITRUST has another set that could range from 150 controls/requirements to 500+ security controls/requirements.

To demonstrate compliance with these standards, it is important to have a deep understanding of (i) exactly which aspects of each control are covered by Azure, (ii) how to implement technical solutions for the other controls that integrate seamlessly with the Azure controls, and (iii) what kinds of responses, processes, and evidence will satisfy auditors.

Project Hosts documents all of the control responses in its ISMSCloud tool. For each HIPAA, NIST 800-66 and HITRUST control, a technical response is provided that is consistent with the Azure Managed Services that Project Hosts is providing. In addition, many controls link to relevant policies or screenshot evidence of controls actually being in place. This allows third-party auditors to efficiently verify compliance with each control.