**Azure Infra Provisioning**

**HIPAA Compliance Standard for HealthCare projects**

|  |  |  |
| --- | --- | --- |
|  | **Prepared By / Last Updated By** | **Reviewed By** |
| **Name** | Nagarajan M – Cloud Architect  Anirudh KC – Cloud Engineer | Ramakrishnan Madhan – Senior Manager |
| **Practice** | CCS | CCS |
| **Date** | 9-Jan-17 | 9-Jan-17 |

**Table of Contents**

Contents

[**1.** **Objective** 3](#_Toc471759965)

[**2.** **HIPAA Guideline Source** 3](#_Toc471759966)

[**3.** **Microsoft Azure HIPAA/HITECH Act Compliance** 3](#_Toc471759967)

[**4.** **Signing a Microsoft Business Associate Agreement (BAA)** 4](#_Toc471759968)

[**5.** **General HIPAA Compliance Guidelines for Azure HC projects** 4](#_Toc471759969)

[**6.** **HIPAA Compliance – Claimsphere Health Care Project** 5](#_Toc471759970)

# **Objective**

The purpose of this document is to provide the basic HIPAA Compliance guidelines to be followed for Healthcare project during Azure Infra provisioning.

# **HIPAA Guideline Source**

Reference

|  |  |  |
| --- | --- | --- |
| # | Source | Link |
| 1 | **Microsoft** | <http://download.microsoft.com/download/8/4/8/8483b6a9-1865-4d17-b6f1-5b66d5c29b10/windows%20azure%20hipaa%20implementation%20guidance.pdf> |
| 2 | **GIS Team** | Mathew Bawol and Tom Corlenius from corporate Security team during HC Internal product (Claimsphere) Azure Infra provisioning project |

# **Microsoft Azure HIPAA/HITECH Act Compliance**

Azure employs a risk-management model of shared-responsibility between the customer and Microsoft. Microsoft is responsible for the platform including services offered, and seeks to provide a cloud service that can meet the security, privacy, and compliance needs of customers. Customers are responsible for their environment once the service has been provisioned, including the applications, data content, virtual machines, access credentials, and compliance with regulatory requirements applicable to their particular industry and locale.

It is possible to use Azure in a way that complies with HIPAA and HITECH Act requirements. However, customers are responsible for determining if the Azure services and the particular applications they intend to run in Azure comply with HIPAA and HITECH Act requirements. Microsoft does not analyze customer data or applications deployed in Azure.

The following Azure features are in scope for the HIPAA BAA:

* Cloud Services (web and worker roles)
* Virtual Machines (including with SQL Server)
* Storage (Blobs, Tables, Queues)
* Virtual Network, Traffic Manager
* Web Sites
* BizTalk Services
* Media Services
* Mobile Services
* Service Bus
* Multi-Factor Authentication
* Active Directory
* SQL Database, and any other features identified as included on the Azure Trust Center

# **Signing a Microsoft Business Associate Agreement (BAA)**

To help comply with HIPAA and the HITECH Act, a customer may sign a written agreement with Microsoft called the **Business Associate Agreement (BAA)**. Microsoft currently offers the BAA only to its Enterprise Agreement (volume licensing) customers and only for the services mentioned in Azure HIPAA/HITECH Act Compliance. Customers should contact Microsoft account manager to sign the BAA.

Customers signing the BAA should email **MSO-HIPAA@microsoft.com** with the subscription ID(s) in which PHI data are stored along with HIPAA Administrative Contact to use for HIPAA-related communications.

# **General HIPAA Compliance Guidelines for Azure HC projects**

Guidelines are classified based on Azure Services and listed below

**Network**

1. Designated and allowed traffic should flow between the servers.
2. Routing of traffic with Route Table to prevent direct access to servers which may lead to Security Issues.
3. Site to Site VPN should be designed in such a way of to restrict the direct access to Azure HIPAA environment from the on-premises to protect data security like copying of data or logs to the local computer.
4. Public IP should be assigned on the need basis so as to prevent access for all the servers from the internet.
5. Servers should be logically separated between clients (not customers specifically). i.e. VDI access per business role and justification is only for required access. i.e. BPaaS personnel should only access application BPaaS interface. Not access to the server / data center segment.
6. Dedicated Hypervisors built in accordance with an SCS must exist for any virtualized nodes. (Not possible like AWS (Dedicated VPC) -- have no control over the virtualization layer.)

**Storage**

1. Azure Storage Service Encryption (AES 256 Bit) for Data at Rest and on transit.
2. Azure Security Center Logging for storing of Logs data in Azure.
3. Logging across the environment must include but not limited to:
   1. Database logging
   2. Active directory logging (application, system, and security)
   3. WAN device logging (Layer 3 Devices)
   4. Application logging
   5. All environmental servers and devices must report logs to a centralized SIEM solution.
4. Internal Key Management solutions and corresponding processes pertaining to the lifecycle of keys and/or certificates used within the environment is required.
5. File transfer / related file transfer access for any reason, including file transfers must occur and/or originate from a dedicated file transfer zone. No native file transfers from internet to be permitted.

**Compute**

1. Data Retention of VM Backup is six years for Healthcare providers as per HIPAA Rules.
2. Multi-factor Authentication for all the Authentication request reaching Azure environment.
3. Multi-Factor Authentication (MFA) based jump hosts within dedicated landing / management zones is required to access and/or administer BPaaS system level access.
4. Users in Active Directory should be given only the required privilege to access HIPAA Azure Environment.
5. Antivirus has to be installed in all the server to prevent viruses, worms, backdoors and Trojans.
6. As per the HIPAA rules we have to store the Windows Logs for 6 years. We can use Storage Account to store the logs where hot storage tier for the recent 1 year and remaining logs can be stored in cold storage tier to reduce the expenditure cost.
7. All lower environments must be segmented from the general purpose hosting and Production (customer pod) networks.
8. Internet access is prohibited for any internal production or lower environment servers.

# **HIPAA Compliance – Claimsphere Health Care Project**

Note: No BAA Agreement with Microsoft for Claimsphere.

|  |  |  |
| --- | --- | --- |
| **Control ID** | **Control Requirements** | **Compliance Comments** |
| 1001 | All lower environments must be segmented from the general purpose hosting and Production (customer pod) networks. | Servers are isolated based on functionality by creating subnets within the network and NSG applied on each |
| 1005 | Multi-Factor Authentication (MFA) based jump hosts within dedicated landing / management zones is required to access and/or administer BPaaS system level access. | Dedicated jump server provisioned to connect to the application environment |
| 1010 | Multi-Factor Authentication into all jump servers is required. In AWS environments, this should include controls to restrict access to the AWS Console. | Implemented RBAC to azure services |
| 1011 | Internet access is prohibited for any internal production or lower environment servers. | Machines are domain joined to AD machine and internal DNS created prohibits the internet access |
| 1032 | Servers should be logically separated between clients (not customers specifically). i.e. VDI access per business role and justification is only for required access. i.e. BPaaS personnel should only access application BPaaS interface. Not access to the server / data center segment. | Machines are isolated by subnet and traffic restricted and secured by NSG/Firewall |
| 1013 | Environment hardening i.e. Secure Configuration Standards (SCS's) across the entire environment including: Servers, WAN Devices, Middleware, DBMS's, etc. is required for secure build and documentation purposes. No new technology and/or devices are permitted in any environment without a SCS and security review. | Standard OS hardening done |
| 1008 | Internal Key Management solutions and corresponding processes pertaining to the lifecycle of keys and/or certificates used within the environment is required. | Not Implemented and planning to use Azure Key Vault |
| 1019 | BPaaS / Off-shore work on products, Dev support, Production support, and any other forms of access must imitate and traverse over secure VDI access into BPaaS. No direct access is permitted. Onshore server access to initiate and traverse only via Jump Hosts via a dedicated management zone. | SSL enabled and all the communication are secured |