Microsoft Azure HIPAA/HITECH Act Implementation Guidance

HIPAA and the HITECH Act are United States laws that apply to most doctors' offices, hospitals, health insurance companies, and other companies involved in the healthcare industry that may have access to patient information (called Protected Health Information, or PHI). In many circumstances, for a covered healthcare company to use a service such as Azure, the service provider must agree in a written agreement to adhere to certain security and privacy provisions set out in HIPAA and the HITECH Act.

This guide was developed to assist customers who are interested in HIPAA and the HITECH Act to understand the relevant capabilities of Azure. The intended audience for this guide includes privacy officers, security officers, compliance officers, and others in customer organizations responsible for HIPAA and HITECH Act implementation and compliance.

While Azure includes features to help enable customers' privacy and security compliance, customers are responsible for ensuring their particular use of Azure complies with HIPAA, the HITECH Act, and other applicable laws and regulations.

Signing a Business Associate Agreement

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 listed in the Scope section below. Customers should contact their Microsoft account manager to sign the BAA.

*Customers signing the BAA **also** must email MSO-HIPAA@microsoft.com to provide the following information: the subscription ID(s) in which you will be storing PHI and the HIPAA Administrative Contact to use for HIPAA-related communications. Please do not use this email alias for any other purpose. We cannot answer questions on HIPAA, signing or reviewing the BAA, how to get in touch with Microsoft, etc. Please email this alias only after you sign the BAA or in the future if you need to update your contact information.*

Prior to signing, you should read this guide and the BAA in full, and evaluate for yourself whether you wish to sign the BAA and place PHI in Azure.

Scope

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.

Storing PHI Data on the Service

Customers should **not** store or process PHI in Azure services outside of the BAA scope unless it is done in a way that renders PHI unusable, unreadable, or indecipherable within that service such that the breach notification requirements of HIPAA and HITECH do not apply. For example, this may be possible if customer encrypts and/or de-identifies the data in compliance with 45 CFR § 164.514(b) and separately stores the identifying/encryption key (for example, off Microsoft's platform or in an Azure service that falls within BAA scope).

Special Considerations

Microsoft strongly recommends that you train your personnel to store PHI only in the objects and data structures designated to for this type of data. **For SQL Database this means**:

Data structures suitable for PHI data:

- Database fields, including BLOBs
- O/S managed through Filestream

Data structures not suitable for storing PHI data:

- Login names
- User Names
- Database names
- Schema names
- Schema Object Names, such as Table Names, View Names, Function Names, or Procedure Names
- Column Names

Recommendations for Enabling 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 our customers. Customers are responsible for their environment once the service has been provisioned, including their 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.

Each customer should have their own compliance mechanisms, policies, and procedures in place to ensure they do not use Azure in a way that violates HIPAA and HITECH Act requirements. Customers should independently verify with their own legal counsel that their implementation meets all HIPAA and HITECH Act requirements.

Azure services in scope for the BAA are audited by independent external auditors under industry standards, including ISO 27001. Our ISO 27001 audit scope includes controls that address HIPAA security practices as recommended by the U.S. Department of Health and Human Services. Additional information on security, privacy, and compliance certifications is available at http://azure.microsoft.com/en-us/support/trust-center/.

Many critical security elements, however, will be determined by applications and systems controlled by the customer. A few specifics that you may wish to evaluate as you design, implement, and operate a customer solution in Azure are:

- **Risk and Security Management:** Microsoft does not monitor the applications and data that customers choose to run in Azure. Thus, to minimize risks to information, you should continuously monitor and log operations in/by guest VMs, Azure Portal, SMAPI, and Azure Storage. This includes monitoring log-in attempts to VMs, RDP access to VMs, applications hosted on Microsoft Azure, and access to storage accounts through various means such as the REST API.

  When using Azure SQL Database, the customer is responsible for identifying, responding to, or mitigating suspected or known incidents that affect or compromise their application with the intent to cause harm to the SQL Database service.

- **Applications and Data:** Critical functionality such as end user access to customer data (including PHI) will be controlled by the design, implementation, and operation of customers' applications. In general, Azure customers are responsible for ensuring the integrity of the information that's written to storage by their applications. For example, customers are responsible for monitoring all application/client level access to their databases to prevent unauthorized access including malicious/accidental changes or deletion of data. Customers should also monitor for security breaches, security incidents, or

impermissible uses and disclosures of PHI that occur within or through your applications or virtual machines.

When using Azure SQL Database, customers are responsible for securing their own applications and clients that access SQL databases in order to prevent unauthorized access. This includes monitoring T-SQL statements executed against their databases through application programs or client-level interfaces for unusual or improper activities (as would be accomplished through application auditing). Customers are also responsible for regular, timely reviews of the audit records they collect as well as any reports and/or alerts they are producing based on those.

Resources on building secure applications are available in the security section of the Azure Trust Center.

- **Configuration of Services:** As a platform service, Azure provides customers with substantial flexibility to configure the features they use, and customers are responsible for doing so in a manner consistent with HIPAA requirements. This is particularly important for configuration of Cloud Services or Virtual Machines. Customers should perform an individualized risk analysis that examines not only the configuration of the Microsoft Azure services they are using but also the management of their accounts, passwords, RDP session settings (such as timeout periods), and security settings on their work stations that access PHI or applications that process PHI. From there, customers should implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level.

- **Access Controls:** Ensuring proper access controls is key to protecting the integrity and privacy of company and patient data. Azure customers are responsible for managing access to VMs, Storage accounts, SQL Databases, the Azure Portal or any other cloud services and resources they use. This includes provisioning and managing Login and User principals for access to their servers and databases respectively (as well as objects within the databases). Logins must be assigned passwords and the customer is responsible for ensuring that their users are aware of their password complexity standards and that they rotate them in a timely manner. Customers must also safeguard their own user identities and credentials (names, passwords, and certificates), other authentication information, and workstations that can be used to gain access to PHI hosted in their service. If a customer believes their access credentials or certificates have been compromised, they should immediately change them and contact Azure Customer Support. Customers are strongly advised to identify and document the roles and responsibilities of their administrators and users who have access to PHI and to institute formal security processes.

- **Redundancy and Backups:** Azure offers a number of features intended to minimize downtime and loss of data. For example, Azure Storage stores multiple copies of data on different fault domains, and, by default, will replicate data to a backup data center (the geo-replication feature can be turned off if desired). Customers are responsible for assessing additional steps to provide added fault tolerance, such as creating additional backups of Customer Data, storing backups of Customer Data off the platform, deploying redundant compute instances within and across data centers, or backing up state within a virtual

machine. Customer should review business continuity options for Azure, located at http://msdn.microsoft.com/en-us/library/windowsazure/hh873027.aspx.

- **Data Center Location:** Customers can configure Azure to use data centers in particular regions and deploy data and applications across multiple data centers for added redundancy. For additional details on the available data centers and data transfer practices, please see the Privacy section of the Azure Trust Center.

- **Encryption-at-Rest:** Microsoft Azure does not automatically encrypt customer data at rest. Customers may implement encryption at rest using .NET cryptographic services.

  For customers using Virtual Machines, additional options are available, including the Encrypting File System in Windows Server 2008 R2 (and above), Azure Rights Management Services, as well as Transparent Data Encryption (TDE) in SQL Server 2008 R2 (and above).

  When using Azure SQL Database, externally encrypted records cannot be queried using T-SQL (other than "retrieve all") and may require a schema change such as the introduction of surrogate keys to enable retrieval of specific records or ranges of records.

- **Encryption-in-Transit:** Customers may configure Azure to enable encryption- in-transit by configuring HTTPS endpoints.

  Customers using Virtual Machines who wish to encrypt traffic between Web clients and Web servers in their VMs can implement SSL on Windows Server Internet Information Services (IIS). Other enhancements to network traffic security include using IPsec VPNs or ExpressRoute to encrypt direct communications between the customer's datacenter and Microsoft Azure. Additional details can be found in the Azure Network Security white paper.

  For Azure SQL Database, all communication to and from SQL Database requires encryption (SSL, TLS 1.1) at all times. For customers who are connecting with a client that does not validate certificates upon connection, the connection to SQL Database is susceptible to "man in the middle" attacks. It is the customer's responsibility to determine if they are susceptible to this type of attack. See the section on "Encryption and Certificate Validation" in the MSDN how-to guide on "Security Guidelines and Limitations (Azure SQL Database)" for details, including how to defend against this type of attack.

- **Personnel:** Customers are responsible for their own employees' training and conduct as it applies to PHI stored in Azure. This may include screening and establishing proper clearance to access certain cloud services, and ensuring authorized personnel's information is kept up to date in Azure.

The above list is not exhaustive and represents just some of the issues to consider in building a HIPAA-compliant solution in Azure. Customers should obtain their own security and legal guidance to ensure their particular use of Azure meets all applicable HIPAA and HITECH requirements.

Customers with specific technical questions may consult Azure Customer Support. Additional technical resources are available at the Azure Developer Center.

Handling Security Incidents

As discussed previously, Microsoft does not monitor for security breaches or other security incidents within customers' applications or virtual machines. Customers are responsible for implementing appropriate monitoring in these and other systems they control. Microsoft does monitor Azure at the platform level, as well as other systems that Microsoft controls.

A Security Incident is any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of PHI or other Customer Data. It does not include Unsuccessful Security Incidents, such as pings and other broadcast attacks on Microsoft's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of PHI or other Customer Data.

Upon becoming aware of a Security Incident involving PHI, Microsoft will report the Security Incident to the administrator(s) of the affected Azure subscriptions. Microsoft will report any information it has developed on PHI involved in a security breach within 30 days of the breach. Microsoft will attempt to provide meaningful information as quickly as possible, to give you time to notify affected individuals. We rely on you (the customer) to handle all notifications to affected individuals.

It is up to you to keep your subscription administrator contact information up to date. Changes can be made within the Azure portal.

Prior to sending a notification, Microsoft will work to contain the breach, analyze its impact, and assess the results. Depending on the nature of the breach, Microsoft may (a) provide you a preliminary notification followed by subsequent details, or (b) wait until a full review has occurred and notify you then. In either case, as stated above, Microsoft will attempt to provide you, within 30 days, sufficient detail for you to understand the security breach's impact on patients, and to fulfill any requirements you may have under HIPAA.

Additional Resources

The following resources are not HIPAA-specific but may assist you in understanding security, privacy, and technical architecture of the service, which can help in planning your HIPAA compliance strategy.

- Azure Trust Center
- Azure Developer Centers
- Azure Customer Support

Disclaimer

This guide is not intended to constitute legal advice. Customers should consult with their own legal counsel regarding compliance with HIPAA, HITECH Act, and other laws and regulations applicable to their particular industry and intended use of Microsoft Azure and other Microsoft products and services. *Microsoft makes no warranties, express, implied, or statutory, as to the information in this document*.