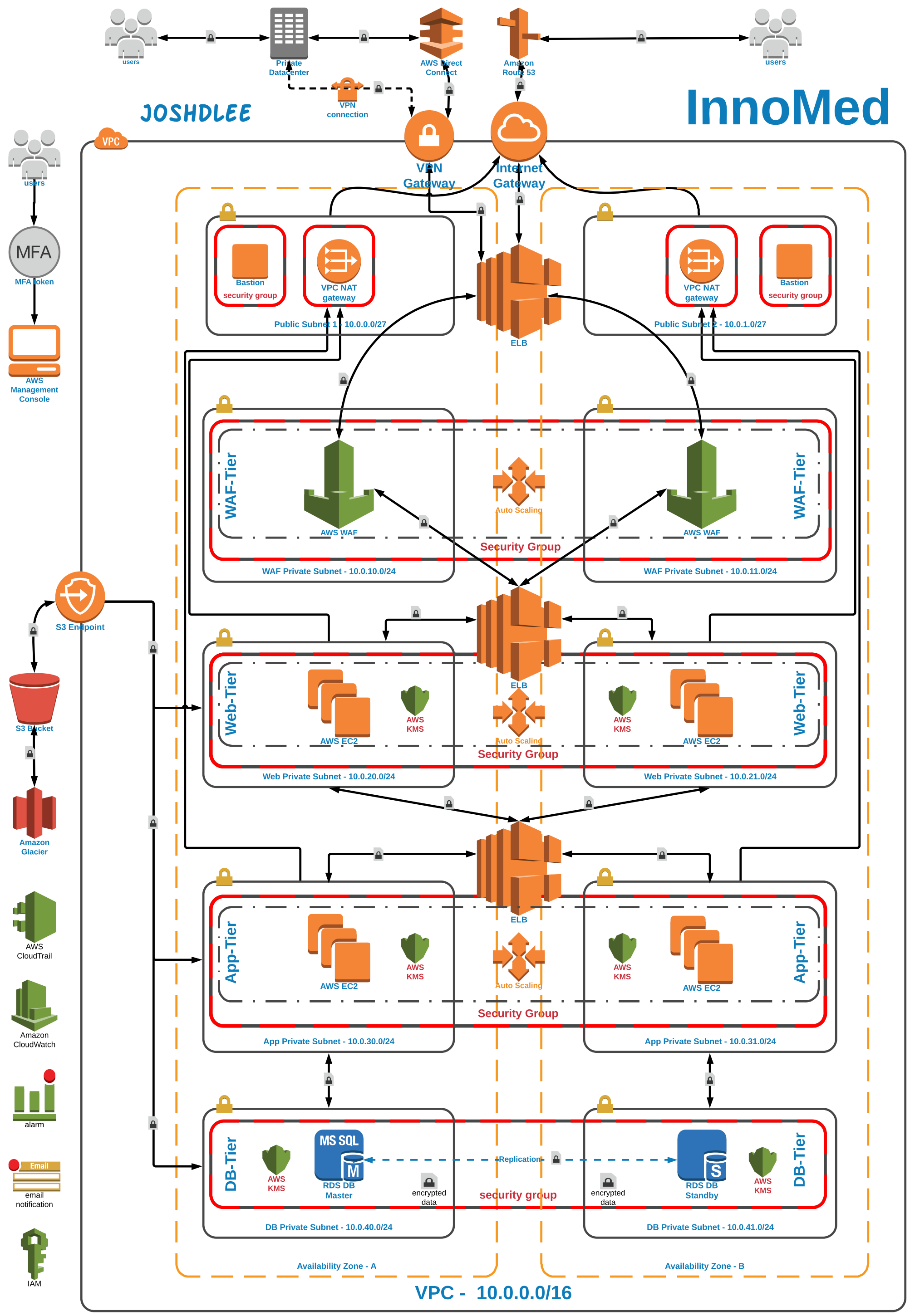

Architecting for HIPAA Security and Compliance on Amazon Web Services

AWS WAF

Web Application Firewall AWS WAF is a web application firewall that helps protect customer web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. Customers may place AWS WAF between their web applications hosted on AWS that operate with or exchange PHI, and their end users. As with the transmission of any PHI while on AWS, data containing PHI must be encrypted while in transit.

Amazon S3

Customers have several options for encryption of data at rest when using Amazon S3, including both server-side and client-side encryption and several methods of managing keys. Connections to Amazon S3 containing PHI must use endpoints that accept encrypted transport (HTTPS). Customers should not use PHI in bucket names, object names, or metadata because this data is not encrypted using S3 server-side encryption and is not generally encrypted in client-side encryption architectures.

Amazon Glacier

Amazon Glacier automatically encrypts data at rest using AES 256-bit symmetric keys and supports secure transfer of customer data over secure protocols. Connections to Amazon Glacier containing PHI must use endpoints that accept encrypted transport (HTTPS). Customers should not use PHI in archive and vault names or metadata because this data is not encrypted using Amazon Glacier server-side encryption and is not generally encrypted in client-side encryption architectures.

Elastic Load Balancing

Customers may use Elastic Load Balancing to terminate and process sessions containing PHI. Customers may choose either the Classic Load balancer or the Application Load Balancer. Because all network traffic containing PHI must be encrypted in transit end-to-end, customers have the flexibility to implement two different architectures:

Customers can terminate HTTPS, HTTP/2 over TLS (for Application), or SSL/TLS on Elastic Load Balancing by creating a load balancer that uses an encrypted protocol for connections. This feature enables traffic encryption between the customer’s load balancer and the clients that initiate HTTPS, HTTP/2 over TLS, or SSL/TLS sessions, and for connections between the load balancer and customer back-end instances. Sessions containing PHI must encrypt both front-end and back-end listeners for transport encryption. Customers should evaluate their certificates and session negotiation policies and maintain them consistent to the Guidance.

Alternatively, customers can configure Amazon ELB in basic TCP-mode (for Classic) or over WebSockets (for Application) and pass-through encrypted sessions to back-end instances where the encrypted session is terminated. In this architecture, customers manage their own certificates and TLS negotiation policies in applications running in their own instances. In both architectures, customers should implement a level of logging which they determine to be consistent with HIPAA and HITECH requirements.

Amazon EC2

Amazon EC2 is a scalable, user-configurable compute service that supports multiple methods for encrypting data at rest. For example, customers might elect to perform application or field-level encryption of PHI as it is processed within an application or database platform hosted in an Amazon EC2 instance. Approaches range from encrypting data using standard libraries in an application framework such as Java or .NET; leveraging Transparent Data Encryption features in Microsoft SQL or Oracle; or by integrating other thirdparty and software as a service (SaaS)-based solutions into their applications. Customers can choose to integrate their applications running in Amazon EC2 with AWS KMS SDKs, simplifying the process of key management and storage. Customers can also implement encryption of data at rest using file-level or full disk encryption (FDE) by utilizing third-party software from AWS Marketplace Partners or native file system encryption tools (such as dm-crypt, LUKS, etc.).

Network traffic containing PHI must encrypt data in transit. For traffic between external sources (such as the Internet or a traditional IT environment) and Amazon EC2, customers should use industry-standard transport encryption mechanisms such as TLS or IPsec virtual private networks (VPNs), consistent with the Guidance. Internal to an Amazon Virtual Private Cloud (VPC) for data traveling between Amazon EC2 instances, network traffic containing PHI must also be encrypted; most applications support TLS or other protocols providing in transit encryption that can be configured to be consistent with the Guidance. For applications and protocols that do not support encryption, sessions transmitting PHI can be sent through encrypted tunnels using IPsec or similar implementations between instances.

Amazon RDS for SQL Server

RDS for SQL Server supports storing PHI for the following version and edition combinations:

- 2008 R2 - Enterprise Edition only
- 2012, 2014 and 2016 - Web, Standard and Enterprise Editions

In order to store PHI, customers must ensure that the instance is configured to encrypt data at rest, and enable transport encryption and auditing, as detailed below.

Encryption at Rest

Customers can encrypt SQL Server databases using keys that customers manage through AWS KMS. On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted consistent with the Guidance in effect at the time of publication of this whitepaper, as are automated backups, and snapshots. Because the Guidance might be updated, customers should continue to evaluate and determine whether Amazon RDS for SQL Server encryption satisfies their compliance and regulatory requirements. Customers using SQL Server Enterprise Edition may choose to use Server Transparent Data Encryption (TDE) as an alternative. This feature automatically encrypts data before it is written to storage and automatically decrypts data when the data is read from storage.

Transport Encryption

Connections to Amazon RDS for SQL Server containing PHI must use transport encryption provided by SQL Server Forced SSL. Forced SSL is enabled from within the parameter group for Amazon RDS SQL Server.

Auditing

RDS for SQL Server instances that contain PHI must have auditing enabled. Auditing is enabled from within the parameter group for Amazon RDS SQL Server.

Using AWS KMS for Encryption of PHI

Master keys in AWS KMS can be used to encrypt/decrypt data encryption keys used to encrypt PHI in customer applications or in AWS services that are integrated with AWS KMS. AWS KMS can be used in conjunction with a HIPAA account, but PHI may only be processed, stored, or transmitted in HIPAA Eligible Services. AWS KMS is normally used to generate and manage keys for applications running in other HIPAA Eligible Services. For example, an application processing PHI in Amazon EC2 could use the GenerateDataKey API call to generate data encryption keys for encrypting and decrypting PHI in the application. The data encryption keys would be protected by customer master keys stored in AWS KMS, creating a highly auditable key hierarchy as API calls to AWS KMS are logged in AWS CloudTrail. PHI should not be stored in the Tags (metadata) for any keys stored in AWS KMS.

Solutions Architect - Professional