ARMOR AUTOMATED COMPLIANCE – HIPAA (HOW TO GUIDE)

PRODUCT MARKETING

FEBRUARY 2019

CONFIDENTIAL DO NOT DISTRIBUTE
Welcome Armor Family!

Thank you for choosing to utilize Armor’s Automated Compliance Solution for HIPAA. This Solution is meant to help our clients more easily achieve HIPAA compliance in the cloud. Armor has used its years of compliance experience helping companies implement HITRUST guidelines in the cloud to achieve HIPAA and combined that with our partnership and experience with AWS to develop this “infrastructure and security-as-code” solution. This solution is a **CloudFormation Template**.

Our CloudFormation Template allows customers to reliably and consistently spin up the basic client/server architecture necessary to run web applications in AWS in a way that is in-line and consistent with the HITRUST guidelines for implementing HIPAA in the cloud. This allows our clients’ developers to move at the speed of modern DevOps shops, while staying in-line with our clients’ security and compliance concerns.

This document acts as a guide to help walk you through the process of installing the template! If you have any questions feel free to reach out to Armor Support!

Cheers,

Your Armor Team
ARMOR AUTOMATE COMPLIANCE – HIPAA (THE SOLUTION)
ARMOR AUTOMATED COMPLIANCE

AWS Cloud

Development / Production VPC

Availability zone

us-east-1b

us-east-1c

Private Subnet

Private Subnet

Private Subnet

Auto Scaling group

Log Collector

AWS CloudWatch

Amazon CloudWatch

AWS Config

CloudTrail

Alarm

Archive Logs

Bucket

S3 Lifecycle Policies to Amazon Glacier

ARMOR AUTOMATED COMPLIANCE
WHAT DOES CFT FOR HIPAA COMPLIANCE ENTAIL?

IMPORTANT:
Armor does not provide legal or compliance advice. Clients are solely responsible for determining and complying with their obligations under HIPAA, the Armor or AWS Business Associate Addendum (BAA), and all other applicable laws, rules and regulations. Clients should consult with qualified legal counsel or consultants, as needed, to ensure that their use of AWS complies with HIPAA, the terms of the AWS BAA, and other applicable laws, rules, and regulations. The information contained in this CloudFormation package is not exhaustive, and must be reviewed, evaluated, assessed, and approved by the customer in connection with the customer’s particular security features, tools, and configurations.
INSTALLING THE CLOUDFORMATION TEMPLATE
WHAT IS CLOUDFORMATION AND HOW DOES IT WORK?

Create a new template
Template-based infrastructure as code that gives AWS a set of instructions to provision and configure a set of resources

Save locally or in S3 bucket
Master template with a series of sub-templates

Create a stack based on your template
Stacks daisy chain the various JSON instructions together in a specified order for resource deployment
HOW DOES CLOUDFORMATION WORK? – CREATING TEMPLATE

- Templates are JSON files (we have already created one for you!!)

- You can find the template link at https://s3.amazonaws.com/armor-hipaa-qs/main.template

- They describe a set of resources for AWS to go provision and any configurations to go with those resources

- For example, the template example to the right here provisions an EC2 Instance for the customer and asks them to specify the KeyPair to SSH into the instance as a parameter.
First, sign into your AWS Console and navigate to the CloudFormation Service. Then click the **Create Stack** button.
After you click Next, you will want to select the following Options: Template is ready, Amazon S3 URL, and enter the URL as shown here. You can then click Next.
This next screen walks you through several Parameter configurations for this CloudFormation Template.

1. Choose your Stack Name. This can be any unique identifier that makes sense for your business.
2. Next, enter a DB password and notification email. This will be the email address by which you receive CloudWatch alerts and alarms.
3. If you have setup AWS Config in the region you’ve selected, then select True, otherwise select False.
4. Pick the Availability Zones you want this CloudFormation Template to be deployed in and failover to.
5. Enter your Armor License Key
   a. If you are already an Armor client, you can find this in AMP.
6. The other parameters should be filled in by default for you!
7. Click Next
Add any tags you want to identify these resources on the next page. "Compliance, Armor, HIPAA" are all examples of tags you might possibly want to use. Next, identify any IAM permissions you want to grant this CloudFormation Template. Armor recommends granting administrative access IAM permissions to this template. However, if you'd like to only specify the exact IAM permissions needed, we can provide them. You can ignore the Advanced Stack options at the bottom of the page. Click Next.
After you review your selections from the previous pages, you will need to acknowledge the CloudFormation permissions to do certain things. A) Create IAM roles and resources and B) auto-expand for scaling purposes. Click **Create Stack** to finish the process and you are done!
THANK YOU!