



# AWS Healthcare Competency

## Consulting Partner Validation Checklist

January 2019  
Version 3.0



This document is provided for informational purposes only and does not create any offer, contractual commitment, promise, or assurance from AWS. Any benefits described herein are at AWS's sole discretion and may be subject to change or termination without notice. This document is not part of, nor does it modify, any agreement between AWS and its customers and/or APN Partners.

# Table of Contents

<b>INTRODUCTION .....</b>	<b>3</b>
<b>EXPECTATIONS OF PARTIES.....</b>	<b>3</b>
<b>AWS HEALTHCARE COMPETENCY PROGRAM PREREQUISITES .....</b>	<b>4</b>
<b>AWS HEALTHCARE CONSULTING PARTNER VALIDATION CHECKLIST .....</b>	<b>7</b>
1.0 Healthcare Practice Overview.....	7
2.0 Operational Excellence .....	8
3.0 Security .....	11
4.0 Reliability .....	14
5.0 Performance Efficiency .....	15
6.0 Cost Optimization .....	<b>Error! Bookmark not defined.</b>
7.0 Healthcare Compliance .....	17

## Introduction

The goal of the AWS Competency Program is to recognize APN Partners who demonstrate technical proficiency and proven customer success in specialized solution areas. The Competency Partner Validation Checklist is intended for APN Partners who are interested in applying for AWS Competency. This checklist provides the criteria necessary to achieve the designation under the AWS Competency Program. APN Partners undergo an audit of their capabilities upon applying for the specific Competency. AWS leverages in-house expertise and a third-party firm to facilitate the audit. AWS reserves the right to make changes to this document at any time.

## Expectations of Parties

It is expected that APN Partners will review this document in detail before submitting an application for the AWS Competency Program, even if all of the prerequisites are met. If items in this document are unclear and require further explanation, please contact your Partner Development Representative (PDR) or Partner Development Manager (PDM) as the first step. Your PDR/PDM will contact the Program Office if further assistance is required.

When ready to submit a program application, APN Partners should complete the Partner Self-Assessment column of the AWS Competency Program Validation Checklist set forth below in this document.

To submit your application:

1. Log in to the [APN Partner Central](https://partnercentral.awspartner.com/) (<https://partnercentral.awspartner.com/>), as Alliance Lead
2. Select "View My APN Account" from the left side of the page
3. Scroll to "Program Details" section
4. Select "Update" next to AWS Competency you wish to apply for
5. Fill out Program Application and Click "Submit"
6. Email completed Self-Assessment to [competency-checklist@amazon.com](mailto:competency-checklist@amazon.com)

If you have any questions regarding the above instructions, please contact your APN Partner Development Representative/Manager.

AWS will review and aim to respond back with any questions within five (5) business days to initiate scheduling of your audit or to request additional information.

APN Partners should prepare for the audit by reading the Validation Checklist, completing a self-assessment using the checklist, and gathering and organizing objective evidence to share with the auditor on the day of the audit.

AWS recommends that APN Partners have individuals who are able to speak in-depth to the requirements during the audit. The best practice is for the APN Partner to make the following personnel available for the audit: one or more highly technical AWS certified engineers/architects, an operations manager who is responsible for the operations and support elements, and a business development executive to conduct the overview presentation.

# AWS Healthcare Competency Program Prerequisites

AWS Healthcare Competency Partners have demonstrated success in building solutions for healthcare payers and providers that securely store, process, transmit, and analyze health data. Working with these Competency Partners gives you access to innovative, cloud-based solutions that have a proven track record handling clinical data and other health information.

Vertical AWS Competencies are designed for APN Partners with *\*segment-specific\** solutions and practices on AWS. These are specialized APN Partners with extensive expertise and experience focused on a specific market segment. APN Partners with highly targeted solutions to industry-specific challenges and consulting practices that offer a unique segment domain knowledge are best positioned to pursue Vertical AWS Competencies. This especially applies to heavily regulated vertical segments, such as Healthcare, Financial Services, and Government where solutions must be specifically tailored for compliance, security, and governance regulations.

The following items will be validated by the AWS Competency Program Manager. Missing or incomplete information must be addressed prior to scheduling of the validation review.

1.0 APN Program Requirements		Met Y/N
<b>1.1 Program Guidelines</b>	The APN Partner must read the Program Guidelines and Definitions before applying to the Healthcare Competency Program. <a href="#">Click here for Program details</a>	
<b>1.2 Consulting Partner Tier</b>	APN Partner must be Advanced or Premier APN Consulting Partner before applying to the Healthcare Competency Program.	
<b>1.3 AWS Certified Personnel:</b>	In addition to the AWS training and certification requirements for the APN Partner's tier, APN Partner must have the following number of certified personnel in relation to their company size:  AWS-Certified Solution Architects at the Professional level: <ul style="list-style-type: none"> <li>▪ ≥ 10 for ≥200 employee company, ≥25 for ≥500 employee company, ≥50 for ≥1000 employee, ≥100 for ≥2000 employee company.</li> </ul>	
2.0 AWS Customer Case Studies		Met Y/N
<b>2.1 Healthcare-Specific Customer Case Studies</b>	<p>APN Partner must have four (4) unique customer case studies specific to completed Healthcare Industry projects on AWS. Two (2) of the four (4) case studies must be publicly referenceable.</p> <p><b>Case studies must be for projects that are in production, rather than in pilot, development or proof of concept stage. Case studies must solve Healthcare line-of-business problems (as defined by AWS) rather than a generic IT problem for a healthcare customer.</b> Each of the four case studies must provide the following information:</p> <ul style="list-style-type: none"> <li>▪ Name of the customer</li> <li>▪ Problem statement/definition</li> <li>▪ What you proposed to solve the problem faced by the customer</li> <li>▪ How AWS services were used as part of the solution</li> <li>▪ How APN Partner's healthcare domain knowledge was used as part of the solution</li> <li>▪ Third party applications or solutions used</li> <li>▪ Project completion must be within the last 18 months</li> <li>▪ Outcomes and results</li> </ul> <p>At least three (3) case studies must incorporate compliance needs as described by their customer.</p> <p>Customer case studies are used to validate your expertise in healthcare solutions in general and in AWS in particular. The customer case studies should highlight the unique value proposition and better-together story of the APN Partner solution running on AWS. This information will be requested as part of the Program Application process in Partner Central.</p>	

<p><b>2.2 Publicly Available Case Studies</b></p>	<p>2.2.1 Two (2) of the four (4) AWS customer case studies must be public; evidence must be in the form of publicly available case studies, white papers, blog posts.</p> <p>2.2.2 Public case studies must be easily discoverable on the Partner’s website, e.g., must be able to navigate and link to the case study from the Partner’s home page.</p> <p>2.2.3 APN Partner must be able to describe the full lifecycle of a Healthcare project:</p> <ul style="list-style-type: none"> <li>▪ Characterization of the business workload (e.g., Compliance, Healthcare Interoperability, Revenue Cycle Management)</li> <li>▪ Identification of toolset, algorithms and software, if any</li> <li>▪ Qualitative and quantitative description of the outcome</li> <li>▪ Performance criterion (minimal acceptable loss, KPIs etc.) and its refresh strategy</li> </ul> <p><i>Note: Public case studies are used by AWS upon approving the APN Partner as a Healthcare Competency Partner to showcase the Partner’s demonstrated success in the practice area and inform customers that Partner has the experience and knowledge needed to develop and deliver solutions to meet their objectives.</i></p> <p><i>Note: For best practice on how to write an accepted Public Case Study <a href="#">See Here</a>.</i></p>	
<p><b>3.0 AWS Healthcare Practice and Focus</b></p>		<p><b>Met Y/N</b></p>
<p><b>3.1 APN Partner Practice Landing Page</b></p>	<p>AWS customers are looking for expertise in the development and delivery of Healthcare solutions on AWS. Therefore, an APN Partner’s internet presence, including webpage layout, specific to their AWS Healthcare Practice helps inform customers about the Partner’s healthcare capabilities and experience.</p> <p>APN Partner must have a landing page that describes their AWS Healthcare Practice, AWS solutions and Competency submitted use cases, technology partnerships, links to AWS customer case studies or case studies, and any other relevant information supporting the Partner’s expertise related to Healthcare and highlighting the partnership with AWS.</p> <p>Healthcare Practice page must be accessible from Partner's home page. Home page is not acceptable as a practice page unless Partner is a dedicated Healthcare consulting company and home page reflects the Partner’s concentration on Healthcare.</p> <p><i>Note: For best practice on how to build an accepted APN Partner Practice Landing Page <a href="#">See Here</a></i></p>	
<p><b>3.2 Healthcare Thought Leadership</b></p>	<p>AWS Healthcare Competency Partners have deep domain expertise in Healthcare, including by developing innovative solutions that leverage AWS services.</p> <p>Specifically, Partner must provide evidence of the ability to communicate and educate customers on processes, vertical-specific use cases, and anti-patterns.</p> <p>APN Partner must have public-facing materials (e.g., blog posts, press articles, videos, etc.) showcasing the APN Partner’s focus on and expertise in Healthcare. Links must be provided to examples of materials published within the last 12 months, examples of customer workshops/education and description of vertical use-cases offered.</p>	
<p><b>3.3 Healthcare Certified Staff</b></p>	<p>Partner must have at least ten (10) employees that have successfully completed the AWS <a href="#">Healthcare Compliance Training</a> for each geography they do business in. For example, if Partner has offices in London and the United States, there must be 10 certified individuals in each of EMEA and North America.</p> <p>APN Partner must present size of technical, non-sales staff focused on healthcare. For practices where this number is below 25, partner must provide public documentation related to the automated capabilities they have built in to scale for healthcare.</p>	
<p><b>3.4 Healthcare Compliance Knowledge</b></p>	<p>APN Partner must present detailed descriptions of the compliance landscape for each geography they do business in. APN Partner must demonstrate process of mapping standards to control frameworks, and provide requisite documentation.</p> <p><i>N.B. This is not an explicit assessment of an APN Partner’s compliance by AWS. Rather, this is intended to gather documentation that the Partner has thought through the practice of mapping their solutions to different regulatory frameworks and that sufficient policies and procedures are in place to meet the concerns of their healthcare customers.</i></p>	

4.0 APN Partner Self-Assessment		Met Y/N
4.1 AWS Competency Partner Program Validation Checklist Self-Assessment	<p>APN Partner must conduct a self-assessment of their compliance to the requirements of the AWS Healthcare Consulting Partner Validation Checklist.</p> <ul style="list-style-type: none"> <li>▪ APN Partner must complete all sections of the checklist.</li> <li>▪ Completed self-assessment must be emailed to <a href="mailto:competency-checklist@amazon.com">competency-checklist@amazon.com</a>, using the following convention for the email subject line: “[APN Partner Name], Healthcare Competency Consulting Partner Completed Self-Assessment.”</li> <li>▪ It is recommended that APN Partner has their Solutions Architect or Partner Development Manager (PDM) review the completed self-assessment before submitting to AWS. The purpose of this is to ensure the APN Partner’s AWS team is engaged and working to provide recommendations prior to the audit and to help ensure a positive audit experience.</li> </ul>	

# AWS Healthcare Consulting Partner Validation Checklist

In preparation for the validation process, APN Partners should become familiar with the items outlined in this checklist and prepare objective evidence, including but not limited to: prepared demonstration to show capabilities, process documentation, and/or actual customer examples. APN Partners are not limited to the four (4) case studies submitted as part of the prerequisite process but should be prepared to describe how the new case studies meet the minimum acceptable criteria for an AWS Healthcare case study if being used during the validation.

The AWS Competency Program is guided by [AWS best practices](#) and [Well Architected Framework](#).

1.0 Healthcare Practice Overview		Met Y/N
<b>1.1 Customer Presentation</b>	<p>APN Partner has a company overview presentation that sets the stage for customer conversations about their AWS Healthcare practice and showcases Partner’s demonstration capabilities.</p> <p>Presentation contains information about the APN Partner’s AWS Healthcare practice, including AWS-specific differentiators, e.g., what is unique about the APN Partner’s Healthcare practice that can only be accomplished leveraging AWS.</p> <p>Overview presentations contain:</p> <ul style="list-style-type: none"> <li>▪ Company history</li> <li>▪ Office locations</li> <li>▪ Number of employees</li> <li>▪ Customer profile, including number and size of customers, including industry</li> <li>▪ Overview of AWS Healthcare Practice</li> </ul> <p>Evidence must be in the form of a presentation delivered by a business development executive at the beginning of the validation session and should be limited to 15 minutes.</p>	
<b>1.2 AWS Healthcare Services Expertise</b>	<p>AWS customers seeking Healthcare consulting services view AWS Healthcare Competency Partners as the go-to experts in the field. Potential customers often ask for examples of solutions built for other customers when choosing an APN Partner and want confidence that partners have knowledge and experience building healthcare solutions on AWS.</p> <p>While each Healthcare workload is unique, security and operations is an underlying theme. For each of the following AWS services:</p> <ul style="list-style-type: none"> <li>▪ AWS CloudTrail</li> <li>▪ Amazon CloudWatch</li> <li>▪ AWS Config and Config Rules</li> <li>▪ AWS CloudFormation</li> <li>▪ AWS Systems Manager</li> <li>▪ AWS Identity and Access Management</li> <li>▪ Amazon GuardDuty</li> <li>▪ AWS Artifact</li> <li>▪ Amazon Inspector</li> <li>▪ Amazon CloudWatch Events</li> </ul> <p>APN Partner can provide the following:</p> <ul style="list-style-type: none"> <li>▪ Examples of customer solutions leveraging each service</li> <li>▪ If the AWS service is not being leveraged by an active customer, a third-party replacement tool (e.g. Terraform for CloudFormation) can be considered with proper evidence and documentation. A hypothetical use case including where that service should be considered and how it will be supported may apply if and only if Partner references do not contain scenarios where said service or 3P equivalent would apply.</li> </ul>	

	<ul style="list-style-type: none"> <li>Description of how services are supported by APN Partner, alone or as part of a solution comprising multiple services</li> </ul> <p><b>Note:</b> Evidence may also be found in the submitted customer case studies (Prerequisites, Section 2.0), AWS Healthcare Practice and Focus (Prerequisites, Section 3.0), during the customer presentation (Section 1.1 above), or during review of other sections.</p>	
<b>1.3 Maintaining AWS Expertise</b>	<p>APN Partner can describe how they stay current on AWS Service releases related to their AWS Healthcare Practice.</p> <p>Evidence must be in the form of a verbal description on enablement materials leveraged by APN Partner to stay current on AWS services and features, as well as training programs they provide employees to stay current, including regular review of the Well-Architected Framework.</p>	
<b>1.4 End of Project Customer Satisfaction Survey</b>	<p>APN Partner asks customer to complete AWS Customer Satisfaction Survey at the end of the project. This is accomplished by searching for the APN Partner in the AWS Partner Solutions Finder and asking Customer to leverage the “Rate this Partner” feature.</p> <p>Evidence must be in the form of a demonstration to show where the “Rate this Partner” feature is located on the AWS Partner Solutions Finder and proof of implementation of this process.</p>	

<b>2.0 Operational Excellence</b>		<b>Met Y/N</b>	<b>Notes</b>
<p>The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include managing and automating changes, responding to events, and defining standards to successfully manage daily operations.</p>			
<b>APN Partner Delivery Model</b>			
<b>2.1 APN Partner Engagement with Customers</b>	<p>APN Partner can describe whether their AWS Healthcare practice delivers only project-based work and hands-off final solution to end customer per terms of the Statement of Work.</p> <p>*or*</p> <p>APN Partner delivers project-based work and retains contractual obligation to the customer to manage and operate Healthcare workloads.</p> <p>Evidence must be in the form of a verbal description or evidence of APN Partner engagement model (e.g., SOWs, SLAs, or MSP contracts) for the customer case studies submitted to meet the Competency prerequisites. Partner must provide documentation (see Section 7.2) of the AWS Business Associate Addendum process (if applicable), how they map healthcare workloads to security standards (e.g. NIST and the HIPAA Security Rule), and how they monitor the environment.</p>		N/A
<b>2.2 MSP Program Participation and Healthcare-Specific Differences</b>	<p>Approved Managed Service Provider (MSP) Partners are subject to a rigorous onsite audit covering the full customer engagement lifecycle and are therefore eligible for waiver of a number of requirements in the following sections.</p> <p>If APN Partner manages workloads and is an approved AWS MSP Partner, APN Partner must describe any differences in their practice as it pertains to supporting Healthcare workloads on an ongoing basis. In particular, APN Partner must provide documentation of the AWS Business Associate Addendum process (if applicable) and how they map healthcare workloads to security standards (e.g. NIST and the HIPAA Security Rule).</p> <p>Evidence must be in the form of a document listing unique considerations for managing Healthcare environments.</p> <p><b>Note:</b> Compliance with this requirement allows APN Partner to claim a waiver for all requirements listed in this Checklist as “Waived if APN Partner is approved AWS MSP.”</p>		N/A

<b>2.3 Customer Handoff and Acceptance for Healthcare Projects (for non-MSP Partners)</b>	<p>If APN Partner performs SoW-only work, APN Partner can describe each phase of the customer handoff and acceptance process.</p> <p>Evidence must be in the form of verbal description, customer training documents, and/or SoW language describing handoff responsibilities.</p> <p>Additionally, APN Partner should demonstrate how they have mapped their developed solution to compliance and regulatory standards, such as NIST and the HIPAA Security Rule.</p>	Not Eligible for Waiver
<b>2.4 Healthcare Certification for Internal Personnel</b>	<p>For SaaS implementations APN Partner has a process to ensure that there are sufficient Healthcare certified personnel to effectively support customers.</p> <p>Evidence must be in the form of:</p> <ul style="list-style-type: none"> <li>▪ An established training plan including on-boarding processes that identify job roles (sellers, solutions architects, project managers) and required training paths. Training plan must include reference to region-specific regulatory frameworks, such as HIPAA or GDPR.</li> <li>▪ A verbal description of methods used to allocate required resources to Healthcare projects</li> </ul>	Not Eligible for Waiver
<b>2.5 Disaster Recovery Planning and Testing</b>	<p>APN Partner demonstrates evidence of disaster recovery planning. For each presented workload, APN Partner can describe the Disaster Recovery process, the recovery-time and recovery-point objectives (RTO/RPO), and provide evidence of planning done in conjunction with the customer.</p> <p>Evidence must be in the form of a documented disaster recovery process, with evidence of testing within the last 12 months.</p>	Waived if APN Partner is approved AWS MSP
<b>2.6 Healthcare-specific Disaster Recovery Considerations</b>	<p>APN Partner has design process to ensure Healthcare solution designs account for how workload will be deployed, updated, and operated.</p> <p>Evidence must be in the form of verbal description and process documentation referring to specific Healthcare customer case studies.</p>	Not Eligible for Waiver
<b>Designing for Operations</b>		
<b>2.7 Business Problem Understanding and Articulation</b>	<p>APN Partner has significant depth in understanding problems that health customers have in specific verticals. This includes providing a set of high-impact line-of-business use cases with quantified business value.</p> <p>Evidence must be in the form of verbal description and process documentation referring to specific Healthcare customer case studies</p>	Not Eligible for Waiver
<b>2.8 Healthcare Design Process: Metrics</b>	<p>APN Partner has implemented Healthcare solutions with performance, service level commitments, marketing, and customer experience objectives.</p> <p>Evidence must be in the form of verbal description, process documentation, and/or technology demonstrations.</p>	Not Eligible for Waiver
<b>Operational Readiness</b>		
<b>2.9 Deployment Checklist</b>	<p>APN Partner uses consistent processes (e.g., checklists) to know when ready to go live with a workload.</p> <p>Evidence must be in the form of completed checklists leveraged for Healthcare solutions.</p>	Waived if APN Partner is approved AWS MSP
<b>2.10 Runbooks/ Playbooks</b>	<p>APN Partner uses runbooks that document routine activities and playbooks that guide the issue resolution process.</p> <p>Evidence must be in the form of runbooks/playbooks for relevant components of Healthcare solutions.</p>	Waived if APN Partner is approved AWS MSP

<b>2.11 Automation through Scripting</b>	<p>APN Partner leverages scripting and tagging to automate execution of runbooks if/where applicable.</p> <p>Evidence must be in the form of script library/demonstration.</p>	<p>Waived if APN Partner is approved AWS MSP</p>
<b>Understanding Operational Health</b>		
<b>2.12 Metrics and Performance Dashboards</b>	<p>APN Partner leverages metrics and performance dashboards to measure operational health (e.g., Amazon CloudWatch Logs, Elasticsearch/Kibana, Personal Health Dashboard, Service Health Dashboard, Third Party solutions).</p> <p>Evidence must be in the form of verbal description and demonstration of operational health metrics/dashboard.</p>	<p>Waived if APN Partner is approved AWS MSP</p>
<b>Responding to Events</b>		
<b>2.13 Planned and Unplanned Event Planning</b>	<p>APN Partner has a process to anticipate operational events, both planned (e.g., sales promotions, deployments, and failure tests) and unplanned (e.g., surges in utilization and component failures).</p> <p>Evidence must be in the form of verbal description with examples of both planned and unplanned events that impacted practice.</p>	<p>Waived if APN Partner is approved AWS MSP</p>
<b>2.14 Healthcare Operations: Event, Incident, and Problem Management</b>	<p>APN Partner has event, incident, and problem management processes, including escalation paths and root cause analysis.</p> <p>Evidence must be in the form of APN Partner demonstration of how events are captured, allocated, escalated, and managed to closure.</p>	<p>Waived if APN Partner is approved AWS MSP</p>
<b>Learning from Experience</b>		
<b>2.15 Lessons Learned</b>	<p>APN Partner demonstrates that lessons learned from each deployment are documented and shared across teams to share the benefits of those lessons.</p> <p>Evidence must be in the form of lessons-learned documentation.</p>	<p>Waived if APN Partner is approved AWS MSP</p>
<b>2.16 Policy as Code</b>	<p>APN Partner has processes and methodologies to conduct AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. If AWS Config is not used, APN Partner can show documented processes and provide technical demonstration of how policies are managed, and the methods used to automate these functions.</p> <p>Evidence must be in the form of technology demonstration and process documentation provided to customer as part of their DevOps conversion.</p>	<p>Not Eligible for Waiver</p>
<b>2.17 Configuration Management</b>	<p>APN Partner has process to automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems. If Amazon EC2 Systems Manager is not leveraged, Partner can show documented processes and provide technical demonstration for how configurations and infrastructure updates are managed, and the methods used to automate these functions.</p> <p>Evidence must be in the form of technology demonstration and process documentation provided to customer.</p>	<p>Not Eligible for Waiver</p>
<b>2.18 Build and Test Code</b>	<p>APN Partner has processes to compile source code, run tests, and produce software packages that are ready to deploy. As part of this process, APN Partner has processes that support provisioning, managing, and scaling servers according to needs. APN Partners may leverage AWS CodeBuild or equivalent.</p> <p>Evidence must be in the form of process documentation describing development and testing processes and examples of how APN Partner teaches customer how to accomplish the same.</p>	<p>Not Eligible for Waiver</p>

3.0 Security		Met Y/N	Notes
The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.			
<b>User Security Best Practices</b>			
<b>3.1 Identity and Access Management</b>	<p>APN Partner has a documented Access Management Strategy and leverages those practices as a key aspect to their DevOps solution for customers, including but not limited to: AWS Identity and Access Management (IAM) users, federated roles, AWS Security Token Service (AWS STS) credentials, access keys, console passwords, and hardware or virtual multi-factor authentication (MFA) devices.</p> <p>Evidence must be in the form of a technology demonstration, process documentation that addresses the above, with context to the submitted customer examples.</p>		Waived if APN Partner is approved AWS MSP
<b>3.2 Protection of Root Account Credentials</b>	<p>APN Partner does not administrate AWS accounts by use of root account credentials.</p> <p>Evidence must be in the form of a technology demonstration.</p>		Waived if APN Partner is approved AWS MSP
<b>3.3 Least Privilege Principle</b>	<p>APN Partner has system that provides access to customer resources to its engineers based on the principle of least privilege. A process for defining and maintaining the appropriate level of access is in place. Access to critical or sensitive data (as defined by the customer) is further controlled by multi-factor or quorum authentication with access-based alerts.</p> <p>Evidence must be in the form of a demonstration of internal capabilities and processes for maintaining least privilege access policies.</p>		Waived if APN Partner is approved AWS MSP
<b>Monitoring and Detection</b>			
<b>3.4 Detective Controls</b>	<p>Activity is monitored appropriately, including by maintenance of logs for capturing performance and security event data, e.g., CloudWatch logs, events, GuardDuty, CloudTrail, VPC Flow Logs, ELB logs, S3 bucket logs, etc.</p> <p>Evidence must be in the form of an example of logs maintained, including demonstration that logs are retained per customer-agreed retention periods.</p>		Waived if APN Partner is approved AWS MSP
<b>Infrastructure and Data Protection</b>			
<b>3.5 Multi-Factor Authentication</b>	<p>APN Partner ensures that multi-factor authentication is activated on all Partner and customer AWS root accounts.</p> <p>APN Partner must show evidence of the use of technology (e.g., AWS Trusted Advisor) for regular auditing of accounts for MFA activation and activation of MFA on new AWS root accounts.</p>		Waived if APN Partner is approved AWS MSP
<b>3.6 Protection of Internal Systems from Attacks</b>	<p>For SaaS Implementations APN Partner has established security policies and procedures to monitor and protect its own systems from attacks.</p> <p>Evidence must be in the form of security policies and procedures</p>		Waived if APN Partner is approved AWS MSP
<b>3.7 Protection of Customer Systems from Attacks</b>	<p>APN Partner has security policies and procedures to help protect its customers' systems from attacks.</p> <p>Evidence must be in the form of security policies and procedures.</p>		Waived if APN Partner is approved AWS MSP
<b>3.8 Communication of Security Best Practices</b>	<p>APN Partner ensures <u>customers</u> understand AWS security processes and technologies as outlined in <a href="https://aws.amazon.com/whitepapers/aws-security-best-practices/">https://aws.amazon.com/whitepapers/aws-security-best-practices/</a>, as may be updated by AWS from time to time.</p>		Waived if APN Partner is approved AWS MSP

	<p>Evidence must be in the form of onboarding and educational documents provided to customers that specifically cover customer security considerations in the APN Partner's environment.</p>		
<b>3.9 Security and Infrastructure Provisioning</b>	<p>Practitioners should have an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion using AWS CloudFormation (or third-party equivalent).</p> <p>Partner has methodologies leveraging standard templated infrastructure provisioning and recommends as a key factor for repeatable deployments to customers wanting to leverage automated Security approaches.</p> <p>Some example of such infrastructure provisioning includes:</p> <ul style="list-style-type: none"> <li>▪ Deploying Security infrastructure, tools, and services across many AWS accounts and regions (firewalls, IDS, proxies, etc.)</li> <li>▪ VPC and Network design. Must including multi-VPC design patterns and multi-region redundancy</li> <li>▪ Designing security infrastructure for secrets management, DDoS Resiliency, Identity and Access Management</li> </ul> <p>Evidence must be in the form of custom deployment templates for four (4) of the submitted customer case studies with description as to whether they encourage use of AWS standardized CF templates, create templates for the customer, or teach customers how to create templates.</p>		Waived if APN Partner is approved AWS MSP
<b>3.10 Centralization</b>	<p>APN Partner and associated case studies must have a processes and methods for providing centralized deployment and management of assets across many AWS accounts, AWS regions, networks, and third-party tools. This centralization must include centralized management of native and third-party tooling, centralization of logging, centralization of identities, and centralization of security alerts/findings</p> <p>Evidence must be in the form of a customer implementation description and must include an architectural diagram and AWS CloudFormation template, where appropriate.</p>		Not Eligible for Waiver
<b>3.11 Inventory, Classification, and Hardening</b>	<p>APN Partner has processes and methodologies to conduct AWS resource inventory, assess current state configuration, review and store historical changes, and send change notifications. By leveraging AWS Config, AWS Inspector, AWS CloudTrail, AWS EC2 Systems Manager, or third-party tools, Partner is able to create remediation plans and provide guidance to enhance a customer's environment by aligning to the principles of the Well-Architected Framework.</p> <p>Partner must show documented processes and provide technical demonstration of how policies are managed, and the methods used to automate these functions.</p> <p>Evidence must be in the form of technology demonstration and process documentation provided to customer as part of their Security conversion.</p>		Not Eligible for Waiver
<b>3.12 ISV and Custom Tooling</b>	<p>Customers have the need to deploy security tools in a scalable manner that will provide operational excellence and not impact the environment. APN Partner must provide a package offering of standardized tools offered to customers and demonstrate how they are deployed and managed. When native AWS tools are not used or are lacking desired features, APN Partner must provide guidance and documentation regarding why a tool was selected and the security outcomes they are achieving with it.</p> <p>Evidence must be in the form of process documentation.</p>		Not Eligible for Waiver
<b>3.13 Infrastructure</b>	<p>APN Partner provides the ability and mechanisms to migrate manual security infrastructure builds and processes into automated, codified, and repeatable</p>		Not Eligible for Waiver

<p><b>and Security as Code</b></p>	<p>processes. APN Partner provides guidance to centralize all standard AWS infrastructure deployment patterns as code stored in a centralized source control repository such as Git. As an example, APN Partner must provide guidance for building out core services such as golden AMI build pipelines, or standard processes of how to update and maintain Security Groups.</p> <p>Evidence must be in the form of process documentation describing software release process and examples of how APN Partner teaches customer how to build and deploy such tasks as an AMI Pipeline or updating/creating AWS Security Groups</p>		
<p><b>3.14 SOC implementation and Incident Response</b></p>	<p>APN Partner can advise on the design, implementation, and enablement of a SOC. Partner provides customers the ability to detect, respond, forensically investigate, and remediate/recover from incidents. APN Partner must have the ability to analyze AWS telemetry including AWS CloudTrail, Amazon GuardDuty Findings, AWS WAF Logs, AWS S3 Access Logs, Amazon VPC Flow Logs, as well as OS and Application logs. APN Partner must have the ability to integrate these security workflows, alerts, and logs into a centralized SIEM and ticketing system.</p> <p>Evidence must be provided in the form of standard IR playbooks and demonstration of automated response plan.</p>		<p>Not Eligible for Waiver</p>
<p><b>3.15 Configuration Drift</b></p>	<p>APN Partner has built mechanisms either for self or customer to detect configuration drift of the environment.</p> <p>Evidence must be provided in the form of templates and scripts to show identification and remediation steps associated with configuration drift.</p>		<p>Not Eligible for Waiver</p>
<p><b>3.16 Application and Operating System Hardening</b></p>	<p>APN Partner can provide industry best practices for hardening and configuring applications and operating systems to industry standards or vendor best practices. As an example, this may be to CIS standards or mandating that an application is only using FIPS-certified software libraries.</p> <p>Evidence must be in the form of automated scripts and/or documentation that includes the processes and steps taken to achieve the hardening.</p>		<p>Not Eligible for Waiver</p>
<p><b>3.17 Solution Delivery Patterns</b></p>	<p>APN Partner has introduced design patterns and security playbooks that help the customer achieve and consistently deliver best practices around the AWS Cloud Adoption Framework (CAF) Core Security Epics of IAM, Logging and Monitoring, Incident Response, Data Protection, and Infrastructure Security which can include such case study examples as:</p> <ul style="list-style-type: none"> <li>▪ Automated deployments of standardized VPCs that meet specific security guidelines (e.g., NIST)</li> <li>▪ Standardized setup of multiple AWS accounts for specific functions (Dev, Test, Prod, Identity, Logging, Security, Shared Services)</li> <li>▪ Standard playbook for identifying and responding to data security breaches, including breaches of PHI under HIPAA (if applicable)</li> <li>▪ Automated deployments of specific application stacks</li> <li>▪ Automated deployments of specific third-party security tools</li> <li>▪ Standardized on-boarding/off-boarding</li> </ul> <p>Evidence must be in the form of a customer implementation description and must include an architectural diagram and AWS CloudFormation template, where appropriate.</p>		<p>Not Eligible for Waiver</p>
<p><b>3.18 Security Tooling</b></p>	<p>APN Partner must have a playbook and design pattern for standardized security tooling they recommend to customers to meet their security and compliance needs, including ALL of the following:</p> <ul style="list-style-type: none"> <li>▪ AWS Account Security Assessment (Root Credential Storage, S3 Bucket Permissions, IAM Permissions, etc.)</li> </ul>		<p>Not Eligible for Waiver</p>

	<ul style="list-style-type: none"> <li>Identity, Access Control, and Federation (Secrets Management, SSO, Privileged User Management, Host/App AuthZ/AuthN)</li> <li>Web Application Firewall (WAF)</li> <li>DDoS protection</li> <li>Firewall and Networking Infrastructure (NGFW, Micro-Segmentation, Security Group Management, Network Analysis/Packet Capture)</li> <li>Remote Connectivity Infrastructure</li> <li>Endpoint, Host Security (EDR/EPP) and Container Security</li> <li>File Integrity Monitoring (FIM)</li> <li>Intrusion Detection and Prevention (IDS/IPS)</li> <li>Centralized Logging, Monitoring, and/or SIEM</li> <li>Proxies and Egress Access</li> <li>Encryption and Key/Secrets Management of S3, EBS, DynamoDB</li> <li>Data Loss Prevention (DLP)</li> </ul> <p>If the tool is NOT part of the AWS Security Competency, APN Partner must provide reasons why the solution was chosen and what mechanisms they have in place to make sure it meets the standards of the Security ISV Competency.</p> <p>Evidence must be in the form of runbooks/playbooks and design patterns for relevant components of aforementioned tooling</p>		
<b>3.19 Encryption of customer content</b>	<p>Customer contact and business/personal information is encrypted on all APN Partner systems including Partner, billing, and ticketing systems.</p> <p>Evidence must be in the form of documentation of customer information storing systems with proof of encryption.</p>		Not Eligible for Waiver
<b>3.20 Encryption at-Rest</b>	<p>APN Partner uses best practices to encrypt all sensitive information at-rest, including protected health information (PHI), at-rest using native AWS encryption capabilities, such as server-side encryption with AWS managed keys or AWS KMS.</p> <p>Evidence must be in the form of documentation, CloudFormation (or equivalent) templates, and environment monitoring capabilities to monitor and remediate any configuration drift and/or services that are out of compliance with their practices.</p>		Not Eligible for Waiver
<b>3.21 Encryption in-Transit</b>	<p>APN Partner uses best practices to encrypt all sensitive information, including protected health information (PHI), in-transit using secure protocols such as HTTPS, IPsec, and SFTP.</p> <p>Evidence must be in the form of documentation, CloudFormation (or equivalent) templates, and environment monitoring capabilities to monitor and remediate any configuration drift and/or services that are out of compliance with their practices.</p>		Not Eligible for Waiver

<b>4.0 Reliability</b>		<b>Met Y/N</b>	<b>Notes</b>
<p>The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.</p>			
<b>Network</b>			
<b>4.1 Service Availability</b>	<p>APN Partner has process to determine service availability needs for customers.</p> <p>See <a href="#">AWS Reliability Pillar whitepaper</a> for specific considerations and guidance on how to calculate service availability with downstream dependencies.</p>		Waived if APN Partner is approved AWS MSP

	Evidence must be in the form of verbal description and/or process documentation.		
<b>4.2 Network Capacity</b>	APN Partner plans network topology for IP-based networks to account for future growth and compatible addressing structures.		Not Eligible for Waiver
	Evidence must be in the form of network growth considerations leveraged for an existing Healthcare customer with accompanying architecture diagram.		
<b>4.3 Network Resiliency</b>	APN Partner plans network topology to ensure the resiliency of connectivity including planning for DDoS attacks, unexpected increase in traffic, or removal of connectivity due to misconfiguration errors.		Not Eligible for Waiver
<b>Application Design for High Availability</b>			
<b>4.4 Application Availability</b>	APN Partner designs applications according to customer needs, factoring in cost of building/maintaining that application to the desired availability levels.		Not Eligible for Waiver
	Evidence must be in the form of verbal description and/or partner documentation leveraged in design process.		
<b>4.5 Service Interruption</b>	APN Partner understands and has processes to automatically remediate common causes of service interruption including but not limited to: hardware failure, deployment failure, load induced interruptions, data induced interruptions, credential expiration, failure of dependent services, infrastructure availability related to power or environmental sources, and/or identifier exhaustion (exceeding available capacity).		Not Eligible for Waiver
	Evidence must be in the form of verbal description how these interruptions are accounted for in customer designs, with description of automated remediation that has been established.		
<b>Testing</b>			
<b>4.6 Testing for Availability</b>	APN Partner uses testing to ensure availability goals are met. This can include but is not limited to: unit testing, load testing, and performance testing, while simulating failure modes while under these tests. Testing should account for dependency unavailability and deployment failures.		Not Eligible for Waiver
	Evidence must be in the form of description of testing and results compared to committed application availability of the application or service.		
<b>Failure Management</b>			
<b>4.7 Root Cause Analysis</b>	APN Partner conducts Root Cause Analysis on failures based on significant events to evaluate the architecture.		Not Eligible for Waiver
	Evidence must be in the form of records of root cause analysis for previous failure with resulting architectural recommendations.		

## 5.0 Performance Efficiency

For this section, APN Partner must select two (2) of the four (4) submitted customer case studies and discuss performance efficiency considerations for both examples.

The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

<b>Customer Case Studies for Performance Efficiency Considerations</b>	<b>[Insert Case Study #1 Here]</b>	<b>[Insert Case Study #2 Here]</b>
--	------------------------------------	------------------------------------

### Selection

<b>5.1 Compute</b>	APN Partner to describe considerations for how it selects the right AWS compute options specifically outlining choice of instances, containers, and functions.		
--------------------	--	--	--

	Evidence must be provided in the form of verbal or written description for submitted customer case studies.		
<b>5.2 Storage</b>	APN Partner to describe considerations for how it selects the right AWS storage options specifically outlining access method, pattern of access, throughput required, frequency of access, frequency of update, and availability and durability constraints.  Evidence must be provided in the form of verbal or written description for submitted customer case studies.		
<b>5.3 Database</b>	APN Partner to describe considerations for how they select the right AWS database options specifically outlining requirements for availability, consistency, partition tolerance, latency, durability, scalability, and query capability.  Evidence must be provided in the form of verbal or written description for submitted customer case studies.		
<b>5.4 Network</b>	APN Partner to describe considerations for how they select the right network options specifically outlining latency, throughput requirements, and location.  Evidence must be provided in the form of verbal or written description for submitted customer case studies.		
<b>5.5 Analytics and Machine Learning</b>	APN Partner to describe considerations for how they select the right AWS analytics and machine learning/artificial intelligence services for their customers specifically outlining requirements for data storage, data representation, and analysis needs.  Evidence must be provided in the form of verbal or written description for submitted customer case studies.		
<b>Performance Monitoring and Review</b>			
<b>5.6 Resource Review</b>	APN Partner has implemented a means of acquiring and preserving source of truth data.  Evidence must be provided in the form of verbal or written description for submitted customer case studies.		
<b>5.7 Performance Monitoring</b>	APN Partner uses techniques to monitor devices after deployment to test the performance and availability.  Evidence must be provided in the form of verbal or written description for submitted customer case studies.		
<b>Performance Tradeoffs</b>			
<b>5.8 Tradeoffs</b>	APN Partner considers tradeoffs during design to ensure an optimal approach for the customer; this may include tradeoffs for consistency, durability, or latency, in order to deliver higher performance.  Evidence must be provided in the form of verbal or written description for submitted customer case studies.		

<b>6.0 Cost Optimization</b>	<b>Met Y/N</b>	<b>Notes</b>
<b>Cost Optimization focuses on avoiding un-needed costs. Key topics include understanding and controlling where money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending.</b>		

Resource Planning			
<b>6.1 Service and Pricing Models</b>	APN Partner considers cost when selecting AWS services, including optimizing by using the most appropriate services.		Not Eligible for Waiver
	Evidence must be in the form of a description of how services and price models are selected for cost optimization.		
<b>6.2 Supply and Demand</b>	APN Partner ensures that capacity matches but does not exceed what is needed, including by using a demand-based, buffer-based, or time-based approach.		Not Eligible for Waiver
	This includes testing for data usage at scale, to account for larger deployments.		
	Evidence must be in the form of a description of capacity planning activities, including testing for demand at scale.		
Cost Optimization over Time			
<b>6.3 Cost Review and Improvement</b>	APN Partner has established a regular cadence to review internal performance and provide recommendations for improvement. Internal optimization involves looking for efficiencies within the APN Partner's operations that result in financial efficiencies, process efficiencies, and/or greater customer satisfaction.		Waived if APN Partner is approved AWS MSP
	Evidence must be in the form of explanation of internal review cadence, and any efficiencies implemented as part of the process (e.g., billing alerts, etc.).		

7.0 Healthcare Compliance		Met Y/N	Notes
Healthcare Compliance focuses on building applications that store, process, and transmit sensitive health-related information, consistent with your privacy and security obligations under frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), Health Information Trust Alliance (HITRUST), Federal Trade Commission (FTC), and Food and Drug Administration (FDA).			
<b>7.1 Controls Mapping</b>	APN Partner has established a standard method for mapping solutions to regulatory standards, such as NIST and or CIS, to help customers determine whether the solutions adhere to applicable regulatory requirements.		Not Eligible for Waiver
	Evidence must be in the form of a controls mapping and/or policy document.		
<b>7.2 HIPAA</b>	7.2.1 APN Partner must provide documentation supporting why their customer solutions do or do not fall under the HIPAA Security, Privacy, or Breach Notification Rules.		Not Eligible for Waiver
	7.2.2 APN Partner can demonstrate knowledge of the current AWS Business Associate Addendum (AWS BAA) by providing the following: <ul style="list-style-type: none"> <li>▪ Description of the AWS BAA</li> <li>▪ Examples of customer solutions leveraging or not leveraging the AWS BAA and the technical safeguards that are put into place to meet AWS BAA requirements, such as demonstrating that protected health information (PHI) is stored, processed, and transmitted only by AWS HIPAA Eligible Services.</li> <li>▪ Familiarity with best practices for configuring AWS HIPAA Eligible Services as set forth in the <a href="#">"Architecting for HIPAA Security and Compliance on Amazon Web Services"</a> whitepaper, <u>as may be updated by AWS from time to time.</u></li> </ul>		

	<ul style="list-style-type: none"> <li>▪ If a current solution requires that a business associate agreement be in place with an active customer, APN Partner must provide a hypothetical use case for when it would be appropriate for the customer to put an AWS BAA in place with AWS directly or alternatively, put a separate business associate agreement in place between the APN Partner and the customer.</li> <li>▪ The APN Partner must demonstrate understanding of the AWS BAA's obligations, and an ability to communicate AWS BAA obligations to their customers if necessary.</li> </ul>		
<b>7.3 GDPR</b>	<p>APN Partner must provide documentation to demonstrate how each customer solution does or does not fall under the General Data Protection Regulation (GDPR).</p> <p>If yes, APN Partner can demonstrate process around how controls described in 7.1 map to GDPR and the responsibilities of data processors and data controllers.</p>		Not Eligible for Waiver
<b>7.4 FTC</b>	<p>APN Partner must provide documentation as to why each of the customer solutions does or does not fall under the FTC Personal Health Record (PHR) regulations.</p> <p>If yes, APN partner demonstrates process around how controls described in 7.1 map to this regulation.</p>		Not Eligible for Waiver
<b>7.5 FDA Medical Device</b>	<p>APN Partner must provide documentation as to why each of the customer solutions does or does not fall under FDA medical device compliance requirements.</p> <p>If yes, APN partner demonstrates process around how controls described in 7.1 map to this regulation.</p>		Not Eligible for Waiver

## AWS Resources

Title	Description
<a href="#">How to Build a Practice Landing Page</a>	Provides guidance how to build a Practice/solution page that will meet the prerequisites of the Program.
<a href="#">How to write a Public Case Study</a>	Provides guidance how to build a Public Customer Case Study that will meet the prerequisites of the Program.
<a href="#">How to build an Architecture Diagram</a>	Provides guidance how to build an architecture diagrams that will meet the prerequisites of the Program.
<a href="#">Partner Readiness Doc</a>	Provides guidance and best practice examples of the Program prerequisites.

*AWS reserves the right to make changes to the AWS Competency Program at any time and has sole discretion over whether APN Partners qualify for the Program.*