Architecting a Compliant Cloud

How Agencies are Tailoring the Cloud for Sensitive Data and Regulated IT Workloads

amazon web services

AWS GovCloud (US)

For government agencies mandated to comply with Federal Risk and Authorization Management Program (FedRAMP), Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) and International Traffic in Arms Regulations (ITAR) requirements, compliance in and security of the cloud remain top priorities.

Today, government agencies and their IT partners are achieving their missions in the cloud without compromising on compliance by leveraging a vetted community approach to cloud adoption. Amazon's AWS GovCloud (US) region was designed as a community cloud isolated from Amazon's other cloud regions, and its IT infrastructure was purpose-built specifically to help government agencies (and their contractors) address their most stringent regulatory and compliance requirements while moving their missions forward with the latest cloud offerings.

The AWS GovCloud (US) region offers an isolated, access-restricted community cloud that is managed by US persons on US soil, and root account credentials are only granted to vetted, US persons working for US organizations. The result is a cloud designed to help customers protect their most sensitive and regulated IT workloads (e.g., Controlled Unclassified Information (CUI)). Beyond the security assurance programs applicable to all AWS regions, AWS GovCloud (US) allows agencies to adhere to CJIS, HIPAA, FedRAMP High, ITAR/EAR, and DoD SRG requirements.

As the customer case studies in this report demonstrate, the AWS GovCloud (US) region may be used for a variety of cloud projects, solutions, and systems including digital image management and streaming, secure data storage and backup, High-Performance Computing and simulations, big data analytics, database services, and citizen services.

Learn more at: https://aws.amazon.com/govcloud-us/.

General Services Administration (GSA) 18F

18F's Cloud.gov Platform Eases Compliance Concerns for Agencies

Cloud.gov, which runs on AWS GovCloud (US) and is built and maintained by 18F, recently received a Provisional Authority to Operate (P-ATO) at the Moderate impact level from the FedRAMP Joint Authorization Board (JAB). It is now the first fully open source FedRAMP solution.

Cloud.gov's mission is to provide a platform as a service for government teams making it faster, simpler, and more secure. The 18F blog post states that, "cloud.gov is for teams that build and deliver websites (and other web-based applications) as part of their work — for example, an agency homepage, an open data API, or an internal information management tool. Your development team sets up the application on cloud.gov, and cloud.gov handles the security, compliance, and maintenance of the underlying platform."

With cloud.gov, government agencies can:

- Quickly deploy applications that comply with federal policies — without needing to manage infrastructure.
- Run scalable cloud-native applications. Since cloud.gov provides services on top of AWS, agencies can take advantage of AWS services, such as Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), and Amazon Elastic Compute Cloud (Amazon EC2).
- Try experiments: build and test prototypes without adding extra expense.
- Shorten the path to ATO (Authority to Operate) for each new or updated application. After an agency issues cloud.gov an ATO, only applications need to be evaluated for security and compliance.

With the recent FedRAMP announcement, now when agencies build a system on cloud.gov, their system or application inherits the FedRAMP compliance of the platform, which substantially reduces the amount of compliance work they need to do and accelerates the path to authorization. It handles many of the FedRAMP technical and compliance requirements of the underlying cloud platform, and allows agencies to focus on their web applications and code instead.

Using AWS removes the necessity of the customer managing this infrastructure. cloud.gov is an optimal solution for small to medium sized agencies seeking a lower barrier to entry for cloud adoption, as well as larger agencies that require streamlined, rapid capability deployment for mission and enterprise applications.

> **"Cloud.gov is for teams that build and deliver websites (and other web-based applications) as part of their work — for example, an agency homepage, an open data API, or an internal information management tool."**
>
> *– GSA web site*

The Electronic Healthcare Network Accreditation Commission (EHNAC) and FIGmd Protect Patient Health Information for Big Data Analysis

FIGmd provides clinical-data registry, analytics, and data-reporting solutions to medical practices, medical professional associations, hospitals, and health systems. The company operates and maintains the largest clinical-data registries in the United States, which customers use to measure, improve, and report healthcare outcomes. FIGmd technologies, solutions, and customization capabilities help organizations scale their projects cost effectively.

Like other healthcare companies, FIGmd is under increasing pressure to demonstrate risk mitigation for transmitting and storing data. "Our customers want us to have third-party review and accreditation/certification so we can show we're meeting industry compliance requirements designed to stop security breaches and cyberattacks," says Sanket Baralay, CEO and founder of FIGmd.

To meet that challenge, FIGmd determined that it needed Electronic Healthcare Network Accreditation Commission (EHNAC) accreditation.

EHNAC's stamp of approval provides objective third-party review of compliance with requirements for the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH,) Affordable Care Act (ACA), and Federal Risk and Authorization Management Program (FedRAMP).

FIGmd was preparing to move its software to a cloud environment. "We wanted to move to the cloud to meet our needs around data storage, scalability, and security," says Baralay, adding that FIGmd needed to ensure EHNAC accreditation was possible in the cloud. "Our customers were concerned about the potential for security vulnerabilities in exchanging and storing healthcare data in the cloud. We needed to find a cloud provider that could work with us on EHNAC accreditation."

In response to the trend of organizations moving to the cloud, EHNAC established a new Cloud-Enabled Accreditation Program (CEAP) so healthcare organizations could receive EHNAC accreditation even after moving to the cloud. CEAP assesses privacy, security, mandated standards, and key organizational functions for organizations

> **"AWS has a great set of services that are FedRAMP authorized, and we reviewed those services before refining our program. As we began shifting our efforts from focusing on physical data center audits to focusing on cloud environments, AWS made us confident the cloud would support healthcare organizations' data exchange under the stringent model we've always followed."**
>
> *- Lee Barrett*

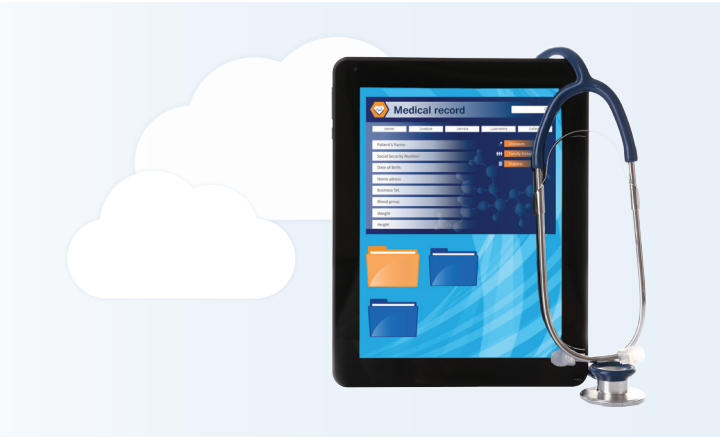
(continued)

running in the cloud. EHNAC announced the program around the same time FIGmd selected Amazon Web Services (AWS) as its cloud provider.

"We chose AWS because its security and scalability capabilities were superior to all the other cloud providers in the market," Baralay says. "EHNAC had announced its support for providers like AWS, so we realized it was the right time to pursue EHNAC accreditation for our new cloud environment."

As a participant in EHNAC's Cloud Service Provider Advisory Committee, AWS worked actively with EHNAC to develop CEAP. "We spent time with the AWS team to discuss the AWS controls around FedRAMP and other regulations," says Lee Barrett, executive director of EHNAC.

"AWS has a great set of services that are FedRAMP authorized, and we reviewed those services before refining our program. As we began shifting our efforts from focusing on physical data center audits to focusing on cloud environments, AWS made us confident the cloud would support healthcare organizations' data exchange under the stringent model we've always followed."



The CEAP program requires organizations meet 74 unique criteria before earning accreditation. In addition to earning its EHNAC CEAP accreditation, FIGmd moved its clinical-data registries to AWS, using Amazon Elastic Compute Cloud (Amazon EC2) instances and storing some customer data in Amazon Simple Storage Service (Amazon S3) buckets. The FIGmd clinical-data registries pull data from different electronic health record systems and give health care organizations the ability to report on compliance.

FIGmd also moved some of its most sensitive clinical-data registry information to AWS GovCloud (US), an isolated AWS region specifically designed to host sensitive data and regulated workloads. Because FIGmd received EHNAC accreditation for workloads on AWS, the company does not need to have data-center inspections and can rely on existing AWS certifications for FedRAMP and other regulations. The organization can now instill a higher level of confidence in customers who are using its clinical-data registries.

"Our customers need to see evidence of our compliance with HIPAA, FedRAMP, and other critical regulations. Having EHNAC accreditation for our AWS workloads helps us demonstrate that compliance," says Baralay. "As a result, our customers can see we're serious about security and privacy and protecting their sensitive health data."

EHNAC is also distinguishing itself by offering CEAP. "As more and more organizations move to the cloud and seek to put risk-mitigation strategies in place, we can play an important role in that process," says Barrett. "We offer the kind of rigorous third-party review and over sight healthcare organizations are looking for, and that provides a greater level of stakeholder confidence."

For FIGmd, being on the AWS Cloud and receiving EHNAC accreditation will likely enable new business growth. "When we engage in conversations with potential customers, it's extremely valuable for us to tell them we can host their sensitive data in the AWS GovCloud and that we have EHNAC cloud accreditation," says Baralay. "That makes our conversations much easier, and ultimately it makes adoption easier for our customers."

Department of Veterans Affairs

Department of Veterans Affairs Protects Patient Data and FISMA High Workloads in the Cloud

In March 2017, the Department of Veterans Affairs (VA) issued Amazon Web Services (AWS) a Federal Information Security Management Act (FISMA) High General Support System Authority to Operate (ATO) for AWS GovCloud (US), as well as a FISMA Moderate GSS ATO for the US East and West Regions.

This validation of a secure environment to run highly sensitive government workloads is important to the VA since they work with patient data, and protecting this data is critical to their mission to make a difference for Veterans. The FISMA High ATO for AWS GovCloud (US) will allow the VA to continue leveraging the cloud to enable their mission.

Moving to the cloud brings many benefits to the VA including:
- Efficient and modern digital experiences
- Cost-savings by provisioning servers on-demand
- Rapid software and product development and deployment cycles
- Modern service-delivery capability
- Zero downtime maintenance windows
- Increased operational flexibility
- Faster identification and resolution of security issues

"We are honored to team with the VA on their journey to the cloud. VA's decision to embrace cloud will have a positive, direct impact on our Veterans, as IT costs are reduced while functionality increases. We look forward to continuing this critical effort with the VA," said Doug VanDyke, General Manager, Civilian Government & Nonprofits, Amazon Web Services Worldwide Public Sector.

"We are honored to team with the VA on their journey to the cloud. VA's decision to embrace cloud will have a positive, direct impact on our Veterans, as IT costs are reduced while functionality increases. We look forward to continuing this critical effort with the VA."

- Doug VanDyke

Jet Propulsion Laboratory (JPL)

NASA's Jet Propulsion Laboratory (JPL) Explores the Cosmos in AWS GovCloud (US)

NASA's Jet Propulsion Laboratory (JPL) is the premier NASA center for the robotic exploration of space. JPL has sent a robot to every planet in the solar system. NASA/JPL is also leading the way in the adoption of cloud computing across the federal government. In fact, cloud computing is an essential part of the tactical operations pipeline for the Mars Science Laboratory mission. From the control room in Pasadena, California, NASA/JPL is using AWS GovCloud (US) to capture and store images and metadata collected from the Mars Exploration Rover and the Mars Science Laboratory missions.

In 2011, NASA launched Curiosity on an 8-month voyage to the Red Planet. This high-profile mission had a number of challenges that needed to be overcome in order to be successful. First, the landing was a huge challenge because Curiosity's mass rendered previous landing approaches untenable. Engineers at JPL designed an innovative entry/descent/landing technique that concluded with a "sky crane" maneuver that gently lowered Curiosity to the surface. NASA wanted to ensure that this thrilling experience was shared with fans across the globe by providing up-to-the-minute details of the mission - especially during the final 7 minutes it took for the rover to descend through the Martian atmosphere and land on Mars. The availability, scalability, and performance of the mars.jpl.nasa.gov website was of the utmost essence during the landing event. Prior to working with AWS, supporting hundreds of thousands of concurrent visitors to the website would have been very difficult, requiring significant web and live video streaming infrastructure that NASA/JPL did not have.

NASA's Jet Propulsion Laboratory used AWS to stream the images and video associated with Curiosity's landing. Cloud computing enabled JPL to provision capacity rapidly and leverage the AWS cloud to deliver successfully engaging experiences of Mars to the public. With public users all over the globe visiting its sites, NASA/JPL served its contents from AWS regions around the world to enhance the viewers experience and scale to meet global demand. Novel use of Amazon Route 53 and Elastic Load Balancers (ELB) enabled NASA/JPL to balance the load across AWS regions and ensure the availability of its content under all circumstances imaginable. The final architecture, co-developed and reviewed across NASA/JPL and Amazon Web Services, provided NASA with assurance that the deployment model could cost-effectively scale, perform, and deliver an incredible experience of landing on another planet. With unrelenting goals to get the data out to the public, NASA/JPL prepared to service hundreds of gigabits/second of traffic for hundreds of thousands of concurrent viewers.

> **"We are honored to team with the VA on their journey to the cloud. VA's decision to embrace cloud will have a positive, direct impact on our Veterans, as IT costs are reduced while functionality increases. We look forward to continuing this critical effort with the VA."**
>
> *- Doug VanDyke*

Resources

- AWS GovCloud (US) FAQs, Pricing and Details: www.aws.amazon.com/govcloud-us
- AWS Compliance Homepage (where you can request security packages and details): https://aws.amazon.com/compliance/
- AWS ITAR Guide: www.aws.amazon.com/govcloud-us/itar
- AWS NIST Quick Starts Guides (automating cloud compliance): https://aws.amazon.com/quickstart/architecture/accelerator-nist/
- AWS Public Sector Summit (there are no registration fees for government employees): https://aws.amazon.com/summits/washington-dc/
- How to Buy Tools for Government Agencies: https://aws.amazon.com/how-to-buy/