ctac

Case Study: Healthcare Case Management System (CMS)

Case Study: Healthcare Case Management System (CMS)

Executive Summary:

CTAC modernized our client's case management systems by migrating from costly, inflexible on-premises infrastructure to a secure AWS cloud environment. The system supports electronic filing (e-filing), digital case file management, and submission of video and audio evidence. CTAC designed a three-tier architecture using AWS services including EC2, RDS, S3, and CloudWatch. The environment is built for high availability, operational resilience, and strict security. Infrastructure is provisioned automatically using Terraform templates stored in version control. Security is enforced through IAM roles, VPC isolation, CloudTrail logging, and encryption with AWS KMS.

The new AWS platform reduced operational costs, improved scalability, and accelerated case processing times. It also enabled the client to support remote digital operations and deliver timely decisions for fraud, compliance, and healthcare appeals.

Introduction to Customer:

CTAC's client within the Department of Health and Human Services (HHS) provides impartial, independent review of disputed decisions in a wide range of HHS programs under more than 60 statutory provisions. The department resolves disputes involving healthcare providers, federal program participants, and other parties seeking administrative review of agency decisions. It handles critical appeals related to Medicare, Medicaid, fraud, healthcare licensing, and regulatory compliance. To fulfill its mission, the Board manages large volumes of sensitive data, including case files, medical records, and investigative materials. The department must meet strict requirements for security, availability, and data integrity, while delivering timely and impartial decisions that impact healthcare programs across the United States.

Customer Challenge:

The Departmental Appeals Board's legacy on-premises infrastructure was aging, costly to maintain, and inflexible. As the volume of electronic filings, case documents, and remote participation increased, the Board needed a modernized platform capable of supporting secure digital operations. The department required a scalable environment that could ensure data security, maintain high system availability, and comply with federal information security standards. Manual processes and rigid infrastructure made it difficult to efficiently handle growing demands for digital case management, video evidence submissions, and remote hearings.

Proposed Solution:

CTAC proposed migrating the department's applications and data to a secure, scalable AWS cloud environment based on a three-tier architecture. The solution leveraged Amazon EC2 for compute resources, Amazon RDS for managed database services, and Amazon S3 for secure document storage. Infrastructure as Code (IaC) principles were implemented using Terraform to standardize environment deployments and support reproducibility across development, staging, and production. To meet strict security and compliance requirements, CTAC incorporated VPC isolation, IAM role-based access control, encryption of data at rest and in transit, CloudTrail audit logging, and automated backup and recovery processes.

Solution Implementation:

CTAC implemented the proposed AWS cloud environment for the department by following a phased, controlled approach. Development and staging environments were deployed first to validate the architecture, security controls, and performance before full production migration. Infrastructure deployment, application migration, monitoring setup, and security configuration were all completed using best practices for reliability, scalability, and compliance.

- **Provisioning and Secure Environment Setup:** CTAC proposed and implemented a secure, three-tier AWS cloud environment for the department using Amazon EC2, Amazon RDS, and Amazon S3. Private VPCs, security groups, and network ACLs were configured to isolate workloads and restrict public access to only necessary endpoints. IAM role-based access controls, CloudTrail logging, and KMS encryption were incorporated to meet federal security and audit requirements.

- **Terraform-Based Infrastructure Management:** All infrastructure was provisioned and maintained using Terraform, stored in version control. Terraform templates ensured reproducibility across dev, staging, and production environments. Changes were applied through manual workflows by authorized system administrators, ensuring traceability and consistency.

- **Modular and Consistent Environment Deployments:** CTAC used standardized Terraform modules and AWS Parameter Store to create modular, environment-agnostic builds. AMIs for application servers were created through Jenkins pipelines and could be deployed across environments without code changes, relying on dynamic configuration injection at runtime.

- **High Availability and Resiliency:** Auto Scaling Groups and Launch Templates were used to ensure instance health and automatic recovery from failures. RDS was deployed in a Multi-AZ configuration for database redundancy and failover support. CloudWatch alarms and health checks were configured to monitor system performance and trigger auto-recovery actions when needed.

- **Monitoring, Backup, and Logging:** Operational monitoring was implemented using Amazon CloudWatch, AWS CloudTrail, and Splunk log aggregation. Daily backups of Amazon RDS were configured via AWS Backup with long-term retention policies. CloudTrail logs were securely stored in a dedicated, access-restricted S3 bucket.

Outcomes and Results:

CTAC successfully migrated the Departmental Appeals Board’s case management systems to a modernized AWS cloud platform.

As a result of the project:

- Reduced operational costs associated with maintaining aging on-premises infrastructure.

- System scalability improved, allowing the department to better handle growing volumes of electronic filings, large case files, and media evidence submissions.

- High availability and automated recovery mechanisms increased system resiliency, minimizing downtime and service disruptions.

- Security posture was enhanced through encryption, VPC isolation, IAM role enforcement, and continuous monitoring via CloudTrail and CloudWatch.

- Remote accessibility and digital case management capabilities were expanded, enabling the department to maintain full operational capacity even during periods of limited physical office access.

These improvements helped our client deliver faster, more reliable decisions in critical fraud, healthcare, and regulatory appeals, strengthening the Board's support of HHS program integrity.

Lessons Learned:

This migration highlighted the value of Infrastructure as Code (IaC) and modular architecture in delivering repeatable, compliant AWS environments at scale.

Early integration of security practices – including encryption, IAM controls, and continuous monitoring – helped streamline the Authority to Operate (ATO) and compliance review processes.

Operational resilience through Auto Scaling and Multi-AZ deployments proved critical to supporting high availability without requiring heavy manual intervention.

Regular validation of backup and recovery processes, along with flexible deployment pipelines, minimized downtime risks during migrations and environment updates.

CTAC's approach reinforced the importance of designing federal healthcare solutions with built-in scalability, security, and operational efficiency from the beginning.