ENPM665-0301

Final Group Project - Group 6

Asmita Samanta (119357408)

Rishi Vyas (119464120)

Ronak Shah (119252987)

“We pledge in our honor that we have not given or received any unauthorized assistance on this exam/assignment.”

**Final Group Project**

**Architectural Design and Overview of Proposed Healthcare Application Platform**

**INDEX**

[Executive Summary 3](#_e7csin7yc6cg)

[Vulnerabilities Count 3](#_srrq6zjz4t6x)

[Vulnerability Chart 3](#_mb95pip21asz)

[**Infrastructure Changes Report 4**](#_fsd3ceczxb5m)

[Vulnerability Assessment 4](#_347mumg4mind)

[Data Security Assessment 5](#_9h0zipa6blhw)

[Virtual Machine Vulnerability Assessment 6](#_b09m33nq99g7)

[Network Security Assessment 7](#_65ok4p7ucuav)

[Disaster Recovery Assessment 8](#_mkzmwzx190on)

[**Services and Methodologies 9**](#_ctwno674aj2g)

[Vulnerability Assessment 9](#_esabykbx26p4)

[Data Security Assessment 11](#_rmw03dnxtqm6)

[Virtual Machine Vulnerability Assessment 15](#_6qml5xto1ca4)

[Network Security Assessment 18](#_3n3fx1vg9vak)

[Disaster Recovery Assessment 19](#_m05rxs9ad5n3)

[**Architecture Diagram 21**](#_hajeo0l2a7dr)

[**Architecture Details - Patient 22**](#_o0clohnmpayd)

[**Architecture Details - Care Provider 24**](#_fsyq6vta30uk)

[**Architecture Details - IT Support 27**](#_19nq3wxk2pvc)

[**References 35**](#_gehmn9bhzohe)

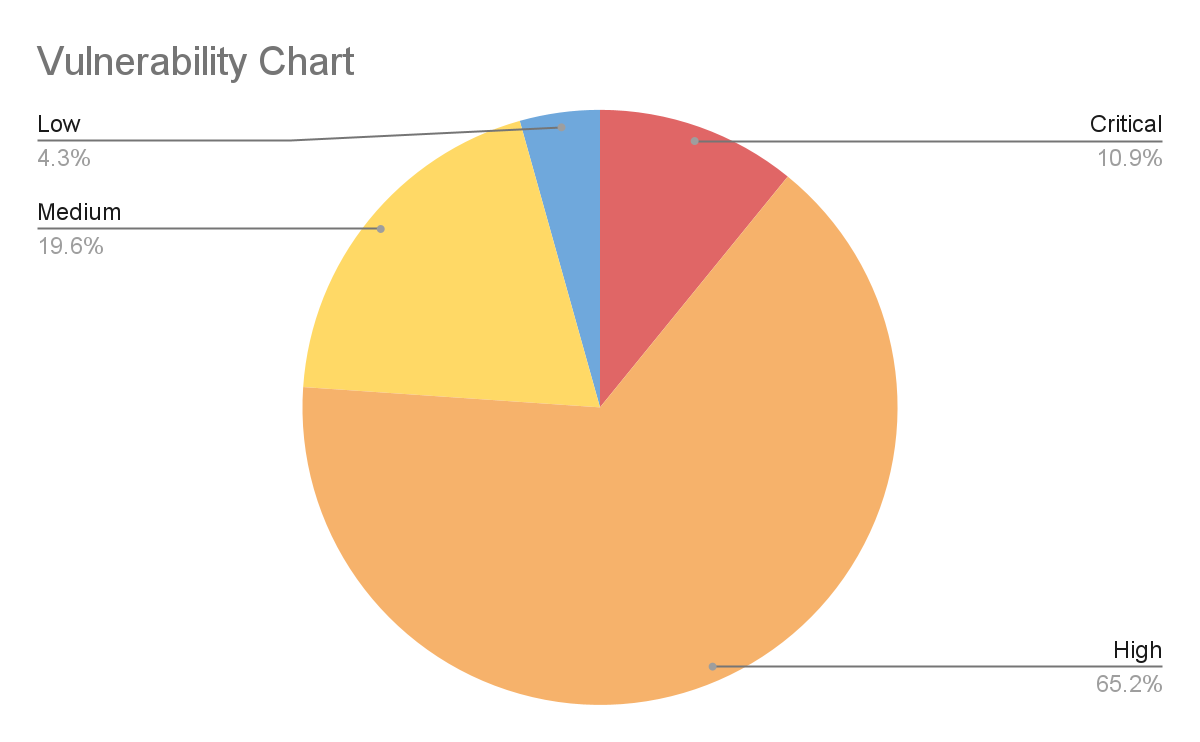
# **Executive Summary**

The purpose of this report is to provide understanding on the fixes implemented and the overview of the architecture employed by the healthcare system and the data flow.

# **Vulnerabilities Count**

| **SL. NO.** | **Severity** | **Fixed Count** | **Not Fixed Count** | **Total Count** |
| --- | --- | --- | --- | --- |
| 1. | **Critical** | 05 | 00 | 05 |
| 2. | **High** | 30 | 00 | 30 |
| 3. | **Medium** | 09 | 00 | 09 |
| 4. | **Low** | 02 | 00 | 02 |
| **TOTAL** | | | | **46** |

# **Vulnerability Chart**

****

## 

### 

# **Infrastructure Changes Report**

| **Vulnerability Assessment** | | | |
| --- | --- | --- | --- |
| **SL NO** | **Name of the Vulnerability** | **Severity** | **Fix** |
| 1 | Missing MFA implementation | Critical | Implemented MFA solutions while enforcing IAM policies and monitoring unsuccessful MFA attempts for all users. |
| 2 | IMDSv2 misconfiguration | High | Implemented IMDSv2 on all instances, additionally, regular review and update of IAM permissions will be carried out using AWS Systems Manager |
| 3 | Missing IAM roles | High | IAM roles have been assigned to an EC2 instance using the Amazon EC2 console |
| 4 | Unencrypted Root volume | High | Utilized Amazon EBS encryption to secure the root volume of an EC2 instance by employing AES-256 data encryption, safeguarding against unauthorized data access. |
| 5 | Unencrypted RDS | High | Enabled encryption for Amazon RDS on the console by choosing the "Enable encryption" option which utilizes AWS KMS keys for resource encryption. |
| 6 | S3 without KMS encryption | High | AWS KMS key encryption has been set up in S3 for sensitive data. |
| 7 | Overly permissive IAM roles | High | Followed the Principle of Least Privilege, which dictates providing each identity, process, or system with the minimum permissions essential for successful task execution. |

| **Data Security Assessment** | | | |
| --- | --- | --- | --- |
| **SL NO** | **Name of the Vulnerability** | **Severity** | **Fix** |
| 8 | Default encryption S3 buckets | High | Employed dual-layer server-side encryption with AWS Key Management Service (AWS KMS) keys (DSSE-KMS) this adds an additional layer of encryption to objects upon their upload to Amazon S3. |
| 9 | Overly permissive IAM policies allowing complete read/write access | High | Reviewed and updated IAM roles to ensure their relevance and effectiveness. |
| 10 | Missing Data Encryption Enforcement for RDS while transit and at rest | High | Encrypt your database storage and backups at rest and transit using Amazon Key Management Service (KMS). |
| 11 | Lack of Regular Backups | Critical | Defined the frequency of backup and implemented incremental backup.  Amazon RDS creates and saves automated backups of your DB instance and Multi-AZ DB cluster during the backup window of your DB instance. |
| 12 | Single Region Infrastructure | High | Deploy multi-region with failover mechanism |
| 13 | No RDS Failover | High | Have more than one region with failover mechanism, RDS backup |
| 14 | No Snapshot Creation | Medium | Implemented regular snapshots of data and tested the backup and restore process regularly. |
| 15 | No Real-Time Monitoring | High | Implemented real time monitoring for infrastructure and applications using CloudWatch metrics and logs |
| 16 | Unencrypted data at rest | High | Encrypt your database storage and backups at rest using Amazon Key Management Service (KMS). |
| 17 | Versioning disabled for S3 bucket | High | Implemented versioning by maintaining multiple variants of an object in S3 bucket. |
| 18 | No bucket access logging | Medium | Enabled Server Access Logging feature for Amazon S3 buckets in order to track access requests useful for security and access audits |
| 19 | Bucket object lock disabled | Medium | Enabled bucket object lock to prevent object from being deleted or overwritten. |
| 20 | Clear text communication allowed by S3 bucket | High | Implemented AWS Macie to mask PII |
| 21 | Overly permissive IAM roles | High | Implemented IAM Access Analyzer |
| 22 | No RDS instance monitoring | High | Implemented RDS monitoring using Amazon Cloudwatch logs, AWS cloud trails and Database activity streams |
| 23 | S3 Bucket with Disabled Server Access Logging | Medium | Enabled using AWS Config |

| **Virtual Machine Vulnerability Assessment** | | | |
| --- | --- | --- | --- |
| **SL NO** | **Name of the Vulnerability** | **Severity** | **Fix** |
| 24 | Weak Authentication and Authorization | Critical | Reviewed the IAM roles and enabled the MFA |
| 25 | Short database credentials | High | Enabled password policy enforcement |
| 26 | Overly permissive Network Rules as Inbound and outbound rules source and destination is set to 0.0.0.0/0 | High | Edit the security groups to allow only the relevant IP addresses.(table) |
| 27 | EBS volumes are not encrypted | High | Encrypted EBS root volumes |
| 28 | No patch management | High | Enabled automated patch policies using systems manager |
| 29 | Unused security group | Low | Removed unused security groups |
| 30 | Not using the latest Linux kernel version | Low | Implemented kernel live patching on Linux2 |
| 31 | Missing security patches | High | Enabled automated patch policies and applied the missing patches using systems manager |

| **Network Security Assessment** | | | |
| --- | --- | --- | --- |
| **SL NO** | **Name of the Vulnerability** | **Severity** | **Fix** |
| 32 | VPCs should be distributed across multiple regions | Critical | Implemented Multi region setup |
| 33 | Poor network segmentation | High | Configured appropriate subnets(public and private) |
| 34 | Weak security group configuration | High | Reviewed and edited the security group rules |
| 35 | No web ACLs created | High | Created Web ACLs |
| 36 | There are no firewall policies | High | Implemented firewall policies |
| 37 | No subnet flow logs | Medium | Enabled VPC flow logs |
| 38 | Route 53 Resolver DNS Firewall Rule Groups Not Configured | High | Route 53 Resolver DNS Firewall Rule Groups Configured |

| **Disaster Recovery Assessment** | | | |
| --- | --- | --- | --- |
| **SL NO** | **Name of the Vulnerability** | **Severity** | **Fix** |
| 39 | No bucket versioning | High | Bucket versioning enabled |
| 40 | Short backup retention period | High | Increased backup retention period |
| 41 | Single region used | Critical | Multi regions implemented |
| 42 | Single AZ RDS instance | High | Multi-AZ RDS instances set up |
| 43 | CloudFormation Termination Protection Disabled | Medium | Enabled Termination Protection |
| 44 | RDS Instance deletion protection is not enabled | Medium | Enabled Deletion Protection for Amazon RDS database instances adds an additional security layer, safeguarding data against unintentional deletions |
| 45 | EC2 Instance Auto Scaling and Deletion Protection Not Enabled | Medium | Configured autoscaling and deletion protection |
| 46 | Lack of Disaster Recovery Plan | High | Multi-site act of failover (critical application) |

# 

# **Services and Methodologies**

## Vulnerability Assessment

1. **Missing MFA implementation:**

* Patients & Care Providers - Patients & Care Providers are entering the AWS Cloud environment using Amazon Cognito and it is typically used to manage user authentication for mobile and web applications. It has MFA, allowing patients & care providers to enroll in the service using a username and password and then choose an additional authentication method, such as SMS text message verification or Time-based One-time Password (TOTP) from an authentication app.
* IT Support - IT support personnel have IAM user accounts to manage AWS resources where IAM policies are enforced to secure access to the AWS Management Console and AWS service APIs. IT support would use their IAM user credentials and MFA as a second factor when signing in, for additional authentication. Any failed authentication attempts will be monitored and logged through AWS CloudTrail and Amazon CloudWatch

1. **IMDSv2 misconfiguration:**

* Patients & Care Providers - While patients & care providers will only interact with the web servers hosted on EC2 instances. They would not interact directly with IMDSv2 on EC2 instances, use AWS Systems Manager, or involve in regular IAM permissions reviews and updates, the security it provides is crucial for safeguarding the underlying infrastructure that hosts patient data and care providers' workflows.
* IT Support - They will ensure that IMDSv2 is correctly configured on EC2 instances when initializing the EC2 instance or modifying the existing ones on which the web servers are hosted to prevent unauthorized access to metadata. They would use AWS Systems Manager to set up routine maintenance tasks on EC2 instances such as patching, compliance enforcement, and automation of manual tasks. They would also be responsible for reviewing and updating IAM permissions to adhere to best practices and maintain security..

1. **Missing IAM roles:**

* Patients & Care Providers - While patients & care providers will not interact with IAM roles directly. The proper system of IAM roles ensures that the backend services they interact with, such as web servers hosted on EC2 instances, have a secure channel to other AWS resources that serve the patient/care provider’s requests. For e.g. A care provider accessing the healthcare application might trigger processes on an EC2 instance that require access to a database or storage service. The IAM role ensures this access is securely managed
* IT support - They are responsible for configuring and managing IAM roles. IT support might also monitor for any signs of misuse or misconfiguration of IAM roles as part of their security and compliance checks.

1. **Unencrypted Root volume:**

* Patients & Care Providers - While patients & care providers will not be involved directly with the EBS encryption of root volumes on EC2 instances which protects the data when -
* sensitive data moves within volumes and instances
* sensitive data is stored on the volumes
* encrypted snapshots are created from the encrypted volumes
* encrypted volumes are restored from the encrypted snapshots

They are also not involved in configuring Amazon Macie that uses ML to ensure that any sensitive data in the volumes is safeguarded and compliant with data protection standards like HIPAA, GDPR etc.

* IT support - They are responsible for configuring EBS encryption across the EC2 instances while creating/modifying EC2 instances and volumes. They also have access to the AWS Key Management Service (KMS), which allows for key rotation and other key management functions.They can also audit the IAM policies, ensuring that only authorized personnel can access the keys. Lastly, they also can configure Macie settings through the AWS management console to monitor S3 buckets in a particular region.

1. **Unencrypted RDS:**

* Patients & Care Providers - While patients & care providers will not interact with encryption of RDS instances in AWS management console . Proper encryption ensures that sensitive data at rest inside the database, on the automated backups, read replicas, and snapshots are protected from unauthorized access to comply with regulations like HIPAA , GDPR etc.
* IT support - They are responsible for configuring encryption across the RDS instances while creating or modifying them by creating a snapshot of the unencrypted database and then creating a new RDS instance from this snapshot with encryption enabled. They also have access to the AWS Key Management Service (KMS), which allows for key rotation and other key management functions.They can also audit the IAM policies, ensuring that only authorized personnel can access the keys.

1. **S3 without KMS encryption:**

* Patients & Care Providers - While patients & care providers will not interact with KMS encryption of their data in S3 buckets . Proper encryption ensures that sensitive data at rest inside the S3 buckets is secure and that decryption happens seamlessly when authorized personnel access it, using the keys provided by KMS.
* IT support - They are responsible for configuring encryption for the S3 buckets by choosing AWS Key Management Service key (SSE-KMS) and using the KMS key. This is done through Amazon S3 Dashboard . Before one does this, they have to create the KMS key in AWS Management Console, if not done already, and enable key rotation and other key management functions.They can also audit the IAM policies, ensuring that only authorized personnel can access the keys.

1. **Overly permissive IAM roles:**

* Patients & Care Providers - While patients accessing the system to view their personal health information & care providers to view specific patient records would be authenticated via Amazon Cognito. Under PoLP, patients & care providers would only have access to their own data and they cannot accidentally or maliciously access other patients' data or system configurations.
* IT support - They are responsible for configuring and managing IAM roles in AWS. They have rights necessary to manage the AWS resources such as monitoring and maintaining servers, handling backups etc. as per role privileges. They have more access than patient or care providers to AWS resources but mostly related to maintaining the backend resources, not full administrative rights across AWS accounts.

## Data Security Assessment

1. **Default encryption S3 buckets**

* Patients & Care Providers - When patients upload their data (such as medical records or personal information) to an application or care providers access their patient data, the data would be stored in S3 buckets. As the data is uploaded, it would first be encrypted with an S3-managed key and then re-encrypted with a KMS-managed key. The dual security ensures that their data is secure from unauthorized access due to encryption and that decryption is only done by authorized people with KMS key access.
* IT support - They are responsible for configuring and managing KMS keys through AWS KMS, including rotating, disabling, or deleting keys as needed, and monitoring their use through CloudTrail logs. They would ensure that only authorized users and services have the necessary permissions to use the keys for encryption and decryption operations.They can also configure AWS GuardDuty to ensure that through VPC Flow Logs, CloudTrail event logs, and DNS logs etc. they are able to detect unauthorized or malicious activity.

1. **Overly permissive IAM policies allowing complete read/write access**

* Patients & Care Providers - Patients have access through Amazon Cognito, which handles user authentication and temporary credential issuance for retrieving their health data. They assume an IAM role with limited permissions tailored to the patient's needs to read their personal and health information. For care providers, in a similar fashion as patients, Amazon Cognito allows read-only access to the patient records that they should have access to.
* IT support - Usually they have access to perform their job functions. For example, an IT support person might need access to CloudWatch logs but not to write access to EC2 instances. Some of them are responsible for configuring and managing IAM roles. IT support might also monitor for any signs of misuse or misconfiguration of IAM roles as part of their security and compliance checks.

1. **Missing Data Encryption Enforcement for RDS while transit and at rest**

* Patients & Care Providers - Patients & care providers access the application that uses RDS for storing sensitive patient information. They are not directly involved with encryption on RDS but they definitely benefit from it as it ensures that the sensitive data they access is secure during transit and when stored in RDS databases
* IT support - For data at rest, they are responsible for setting up encryption for new/existing RDS instances using AWS KMS to encrypt the database files on disk, as well as the backups, snapshots, and read replicas associated with the instance. For data in transit, they have to ensure that all connections to the database use SSL/TLS by default. They will ensure that encryption is enforced, audit the encryption status, and respond to any incidents related to security through AWS Config. This is very necessary because sensitive data needs to be secure and encrypted, to be compliant with health data protection regulations such as HIPAA. They also have access to configure IAM policies to control who can manage KMS keys and RDS instances, restricting access to sensitive actions

1. **Lack of Regular Backups**

* Patients & Care Providers - Patients & care providers benefit largely from backups as it ensures their data is safe and can be quickly restored if necessary, maintaining the integrity and availability of critical health information for further services to mankind.
* IT support - They are responsible for setting up and monitoring backups using Amazon RDS. They choose the backup window, set the retention period, and ensure that backups are executed successfully. They use tools like the AWS Management Console to manage these settings, and Amazon CloudWatch to monitor backup events and receive alerts in case of failures. They also configure Multi-AZ deployments of RDS to provide high availability and further data protection, as they allow for a primary DB instance to be replicated synchronously to a secondary instance in a different Availability Zone (AZ).

1. **Single Region Infrastructure**

* Patients & Care Providers - Patients benefit largely from a multi-region infrastructure. They would experience less downtime and potentially faster access to the applications they rely on to access their own health records. For care providers, they can access their authorized set of patient records and further start their care management services.
* IT support - IT support would be responsible for setting up and maintaining the multi-region infrastructure. This includes configuring Amazon Route 53 for traffic routing and failover, implementing database replication across regions Amazon RDS, data synchronization across regions using Amazon S3 replication and monitoring the health and performance of all regions using CloudWatch by setting up alarms and notifications.

1. **No RDS Failover**

* Patients & Care Providers - Patients benefit from a multi-region failover mechanism and RDS backups as it ensures that their access to healthcare applications is uninterrupted, maintaining the availability of critical health services and data . For care providers, they rely on high availability of access to patient data and healthcare applications at any time to further start their care management services.
* IT support - IT Support is responsible for setting up, monitoring, and managing the failover mechanisms. This includes configuring Amazon Route 53 for traffic routing and failover, implementing database replication across regions Amazon RDS and monitoring the health and performance of all regions using AWS CloudWatch and CloudTrail by setting up alarms and notifications.

1. **No Snapshot Creation**

* Patients & Care Providers - Patients and care providers benefit from regular snapshots because it ensures that their sensitive health data is protected against loss. While they do not directly participate in the process, their experience is impacted positively by the increased reliability and security of their data.
* IT support - IT Support is responsible for setting up and managing the backup processes. Through the AWS Management Console, they can create backup plans at their preferred frequency, retention period for resources like RDS instances. For snapshots, one can use AWS Command Line Interface (CLI) and use Amazon CloudWatch to trigger those snapshot creations. Testing for the snapshot creations can be manually done through AWS Management Console or automated through CloudWatch.

1. **No Real-Time Monitoring**

* Patients & Care Providers - Patients indirectly benefit from real-time monitoring because it ensures that the healthcare applications they rely on are highly available and performant. For care providers, monitoring is even more important because any outages can significantly impact their ability to provide further care based on their access to patient information.
* IT support - IT Support is responsible for setting up and managing CloudWatch. They create dashboards to observe the health of the resources and applications, set up alarms for anomaly detection, and ensure that logging is appropriately configured for all services.

1. **Unencrypted data at rest**

* Patients & Care Providers - They typically would not be directly involved in the encryption process. However, they benefit from enhanced data security, which protects their personal and health information from unauthorized access.
* IT support - They are responsible for configuring encryption across the RDS instances using KMS while creating or modifying them by creating a snapshot of the unencrypted database and then creating a new RDS instance from this snapshot with KMS encryption enabled. IT Support has access to the AWS Key Management Service (KMS), which allows for key creation, rotation and other key management functions.They can also audit the IAM policies, ensuring that only authorized personnel can access the keys. They can also configure AWS Inspector that can check for unencrypted resources like RDS instances, helping to identify where data at rest is not encrypted.

1. **Versioning disabled for S3 bucket**

* Patients & Care Providers - They typically would not be directly involved in the versioning process. However, they benefit from enhanced data integrity and security, ensuring their medical records or data are not lost or overwritten. Care providers can use past data for backtracking diseases of patients or researching/developing intensive healthcare for future deadly diseases.
* IT support - They are responsible for implementing and managing versioning in S3.They would use tools such as the AWS Management Console, AWS CLI to enable and configure versioning on S3 buckets when storing data so that any update or delete operation would not result in data loss.They can also set up lifecycle policies to manage the retention and deletion of old versions to control costs.

1. **No bucket access logging**

* Patients & Care Providers - They typically would not be directly involved in the bucket access logging. However, they benefit from enhanced data integrity of health records and other sensitive data they may need to access through the access logging. It ensures that the information they rely on for patient care cannot be altered or deleted, maintaining a reliable source of truth.
* IT support - IT support personnel are responsible for enabling and configuring the Server Access Logging. They would use the AWS Management Console or AWS CLI to apply Server Access Logging settings to the required S3 buckets. They would set up the destination bucket for the logs, define the log format, and establish the appropriate permissions

1. **Bucket object lock disabled**

* Patients & Care Providers - They typically would not be directly involved in the bucket object lock. However, they benefit from enhanced data integrity of health records and other sensitive data they may need to access. It ensures that the information they rely on for patient care cannot be altered or deleted, and is compliant with healthcare regulations like HIPAA.
* IT support - IT support personnel are responsible for enabling and configuring the Object Lock feature. They would use the AWS Management Console or AWS CLI to apply Object Lock settings to the required S3 buckets according to the compliance requirements.They would also manage the permissions to ensure that only authorized personnel can alter the lock settings, through IAM.

1. **Clear text communication allowed by S3 bucket**

* Patients & Care Providers - They typically would not be directly involved in masking PII. However, they benefit from it because it helps ensure that their sensitive data, like health records, is automatically discovered and protected. They also believe on Macie’s ability to secure data by maintaining compliance with health data protection regulations
* IT support - IT support personnel are responsible for setting up and configuring AWS Macie.. They would use the AWS Management Console to manually set it up or AWS CLI to automate the process.

1. **Overly permissive IAM roles**

* Patients & Care Providers - They typically would not be directly involved in IAM Access analyzer. However, they benefit from it because it helps ensure that their sensitive data is not inadvertently exposed due to overly permissive policies.They rely on IT to manage permissions correctly so that they have access to the necessary data without exposing any sensitive information to other unauthorized users.
* IT support - IT support will be performing security audits using IAM Access Analyzer. They would use this tool to check and modify permissions, ensuring that every user, including care providers and potentially patients, has the access they need without excess permissions that could pose a risk.

1. **No RDS instance monitoring**

* Patients & Care Providers - They benefit indirectly from this monitoring because it ensures the security and compliance of the storage services where their personal and health data is stored.
* IT support - They are involved in setting up and managing these monitoring tools. They would configure the CloudWatch Logs for RDS, set up CloudTrail for API auditing, and enable Database Activity Streams for real-time activity monitoring. They would also create CloudWatch Alarms to notify them of any unusual database activities or operational issues that could impact database performance or security

1. **S3 Bucket with Disabled Server Access Logging**

* Patients & Care Providers - They benefit indirectly from this monitoring because it ensures the high availability and security of the databases that store their personal and medical information. AWS Config helps ensure that the systems they use are compliant with security best practices and regulatory standards
* IT support - IT support is involved in configuring the AWS Config. They set up the AWS Config rules, monitor the compliance dashboard, and act on non-compliance notifications. IT support would use AWS Config's dashboard and the AWS CLI or SDKs to manage Config rules and review the resource configurations.

## 

## Virtual Machine Vulnerability Assessment

1. **Weak Authentication and Authorization**

* Patients & Care Providers: Users entering the AWS Cloud environment rely on Amazon Cognito, a service designed to manage user authentication for mobile and web applications. To address the vulnerability, a robust Multi-Factor Authentication (MFA) system has been implemented. Patients & Care Providers can enroll in the service using a combination of a username and password. Additionally, they are empowered to choose an extra layer of authentication, such as SMS text message verification or Time-based One-time Password (TOTP) from an authentication app.
* IT Support: IT support personnel, holding IAM user accounts for the management of AWS resources, adhere to enforced IAM policies regulating access to both the AWS Management Console and AWS service APIs. As a corrective measure, IAM user credentials are coupled with MFA as a second factor during sign-in. This additional authentication layer enhances the overall security posture. In case of any unsuccessful authentication attempts, the system diligently monitors and logs these events through AWS CloudTrail and Amazon CloudWatch.

1. **Short Database Credentials Vulnerability**

* Patients & Care Providers: Patients & Care Providers interacting with the AWS Cloud environment, specifically utilizing AWS Identity and Access Management (IAM) and Relational Database Service (RDS) services, benefit from enhanced security measures addressing the short database credentials vulnerability. Stringent password policies are now enforced, leveraging the capabilities of AWS IAM. This ensures that Patients & Care Providers create and maintain robust passwords, incorporating a combination of uppercase and lowercase letters, numbers, and special characters.
* IT Support: The implementation of robust password policies, enforced by AWS IAM, mandates IT support staff to create and regularly update strong passwords. Regular audits, facilitated through IAM and RDS services, confirm ongoing compliance with these policies. This collective effort reinforces the resilience of the authentication process, minimizing the risk of unauthorized access due to weak credentials. The utilization of AWS IAM and RDS services ensures a comprehensive approach to securing database credentials within the AWS environment.

1. **Overly Permissive Network Rules Vulnerability:**

**Patient & Care Providers:**

* + Implementing AWS Security Groups can enhance the security stance of the AWS resources, reducing the attack surface by limiting unnecessary access. This helps protect patient data and ensure the availability of critical healthcare services. Patient users don’t typically interact with AWS security groups directly, but these rules help protect their data. The IT team can create rules that allow inbound HTTP and HTTPS access to the services that patients use.
  + Implementing AWS Network Firewall can help protect the healthcare services from exploits that originate from IP addresses that are known to be operated by bad actors.
  + AWS Shield provides automatic, always-on detection and inline mitigation to minimize application downtime and latency. This ensures that healthcare services remain available and reachable for patients. AWS Shield helps protect the healthcare services from DDoS attacks, ensuring that these services remain available for patients.
  + AWS WAF helps protect the web applications that patients interact with from common web exploits. AWS WAF provides flexible options for implementing protections, controlling ingress traffic to the application. This helps ensure that the web applications patients use is secure and reliable.

**IT Support:**

* + IT support users can create and manage AWS security groups. They can create rules that control inbound and outbound traffic, and that allow access to specific database ports. Implementing AWS Security Groups can enhance the security stance of your AWS resources, reducing the attack surface by limiting unnecessary access. This helps protect sensitive healthcare data and ensure the availability of critical healthcare services.
  + IT support users can use AWS Network Firewall to deploy essential network protections for all Amazon Virtual Private Clouds (VPCs). Implementing AWS Network Firewall can help protect the healthcare services from exploits that originate from IP addresses that are known to be operated by bad actors.
  + IT support users can manage the implementation of AWS Shield, which provides protection against DDoS attacks. AWS Shield helps protect the healthcare services from DDoS attacks, ensuring that these services remain available.
  + IT support users can manage AWS WAF, which helps protect web applications from common web exploits. AWS WAF provides flexible options for implementing protections, controlling ingress traffic to the application. This helps ensure that the web applications are secure and reliable.

1. **EBS Volumes Not Encrypted Vulnerability:**

* For both user categories utilizing AWS IAM and RDS services, addressing the vulnerability of unencrypted EBS volumes involves identifying and encrypting such volumes, particularly root volumes. Leveraging the AWS Key Management Service (KMS) for encryption adds an extra layer of security. Encrypting EBS volumes is paramount as it safeguards data confidentiality, providing additional protection against unauthorized access to stored information.

1. **No Patch Management Vulnerability:**

* Automated patching processes using AWS Systems Manager is the solution for both Patients & Care Providers and IT Support. This involves the automation of patch application, coupled with regular monitoring and application of patches to maintain overall system security. Automated patch management ensures the timely application of security updates, significantly reducing the risk of vulnerabilities being exploited by malicious actors.

1. **Unused Security Group Vulnerability:**

* Both Patients & Care Providers and IT Support can improve security by conducting a comprehensive audit of security groups and removing any unused groups. This meticulous approach eliminates potential attack vectors by reducing the attack surface. The importance lies in minimizing the risk of unauthorized access through unnecessary configurations, thereby enhancing the overall security posture.

1. **Not Using the Latest Linux Kernel Version Vulnerability**:

* Identifying instances with outdated Linux kernel versions is crucial for both user categories. Implementing live kernel patching on Linux2 addresses this vulnerability by applying security patches without system reboots. The importance of keeping the Linux kernel up to date using live patching cannot be overstated, as it mitigates the risk of known vulnerabilities being exploited by attackers.

1. **Missing Security Patches Vulnerability:**

* Both Patients & Care Providers and IT Support can utilize AWS Systems Manager to enable automated patch policies and apply missing patches. This involves leveraging Amazon Inspector to assess instances for vulnerabilities and ensure compliance. Automated patching, coupled with monitoring, is essential to protect the system against known vulnerabilities, reducing the window of exposure to potential threats.

## Network Security Assessment

1. **VPCs Should Be Distributed Across Multiple Regions Vulnerability**:

* Implementing a multi-region setup is critical for both user categories to enhance fault tolerance. Configuring VPCs in multiple AWS regions for redundancy and disaster recovery, and distributing critical resources across regions, ensures continuous service availability even in the event of regional outages or disasters.

1. **Poor Network Segmentation Vulnerability**:

* Both Patients & Care Providers and IT Support can improve network security by implementing proper network segmentation using public and private subnets. This includes isolating critical resources from public access to minimize attack vectors. Proper network segmentation is crucial to prevent lateral movement in case of a security breach, limiting the impact of potential attacks.

1. **Weak Security Group Configuration Vulnerability**:

* Regularly reviewing and editing security group rules for adherence to the principle of least privilege is crucial for both user categories. Well-configured security groups, with restricted inbound and outbound traffic, reduce the attack surface. This proactive approach prevents unauthorized access and potential exploitation of vulnerabilities.

1. **No Web ACLs Created Vulnerability**:

* Implementing Web Access Control Lists (ACLs) is essential for both Patients & Care Providers and IT Support to filter and control web traffic. Defining rules to allow or deny access based on specific conditions adds an additional layer of defense against web-based attacks, protecting web applications from malicious traffic.

1. **No Firewall Policies Vulnerability**:

* For both user categories, defining and enforcing firewall policies to control incoming and outgoing traffic is crucial. Specifying rules to allow or block traffic based on security requirements adds an essential layer of protection, regulating network traffic and preventing unauthorized access to sensitive resources.

1. **No Subnet Flow Logs Vulnerability**:

* Enabling VPC flow logs is crucial for both Patients & Care Providers and IT Support to capture information about IP traffic within the VPC. Using flow logs for monitoring, troubleshooting, and security analysis provides visibility into network traffic patterns. This aids in the detection of suspicious activities and ensures compliance with security policies.

1. **Route 53 Resolver DNS Firewall Rule Groups Not Configured Vulnerability**:

* Configuring DNS Firewall Rule Groups in Route 53 Resolver is vital for both user categories. This involves controlling DNS traffic by defining rules to block or allow specific domains based on security policies. Configuring DNS firewall rules adds an additional layer of defense against malicious domain resolutions, enhancing overall network security.

## Disaster Recovery Assessment

1. **No Bucket Versioning Vulnerability**:

* Addressing the absence of bucket versioning is imperative for both Patients & Care Providers and IT Support. Enabling versioning for S3 buckets involves maintaining a history of object versions. This allows for the recovery of previous versions in the event of unintended modifications or deletions. The importance lies in providing data resilience and ensuring the integrity of stored information.

1. **Short Backup Retention Period Vulnerability**:

* For both user categories, increasing the backup retention period is crucial. Extending the retention period ensures longer data retention for recovery purposes. Establishing a snapshot backup system at hourly intervals, with storage accommodated for an extensive duration of 100 years, enhances the ability to recover from data loss incidents. This not only ensures business continuity but also minimizes downtime.

1. **Single Region Used Vulnerability**:

* To enhance redundancy and resilience, both Patients & Care Providers and IT Support can benefit from expanding resources and services to multiple AWS regions. Distributing critical workloads across regions ensures improved availability and fault tolerance. Utilizing multiple regions is essential for business continuity, reducing the impact of regional failures and providing a geographically distributed infrastructure.

1. **Single AZ RDS Instance Vulnerability**:

* Configuring RDS instances to operate in Multi-AZ (Availability Zone) mode is vital for both user categories. This enhances database availability and reliability by ensuring continuous access to critical data, even in the event of an Availability Zone failure. Assessing failover scenarios validates the resilience of the architecture, providing a robust solution against potential disruptions.

1. **CloudFormation Termination Protection Disabled Vulnerability**:

* Enabling termination protection for CloudFormation stacks is crucial for both Patients & Care Providers and IT Support. This involves preventing accidental deletions and implementing strict access controls for users authorized to modify or delete stacks. Enabling termination protection is paramount for preserving the stability of deployed resources and preventing critical infrastructure from being unintentionally deleted.

1. **RDS Instance Deletion Protection Not Enabled Vulnerability**:

* Enabling deletion protection for Amazon RDS database instances is essential for both user categories. This adds an additional layer of security against unintentional deletions. Adjusting deletion protection settings based on the organization's policies ensures data integrity by preventing the accidental loss of critical RDS instances.

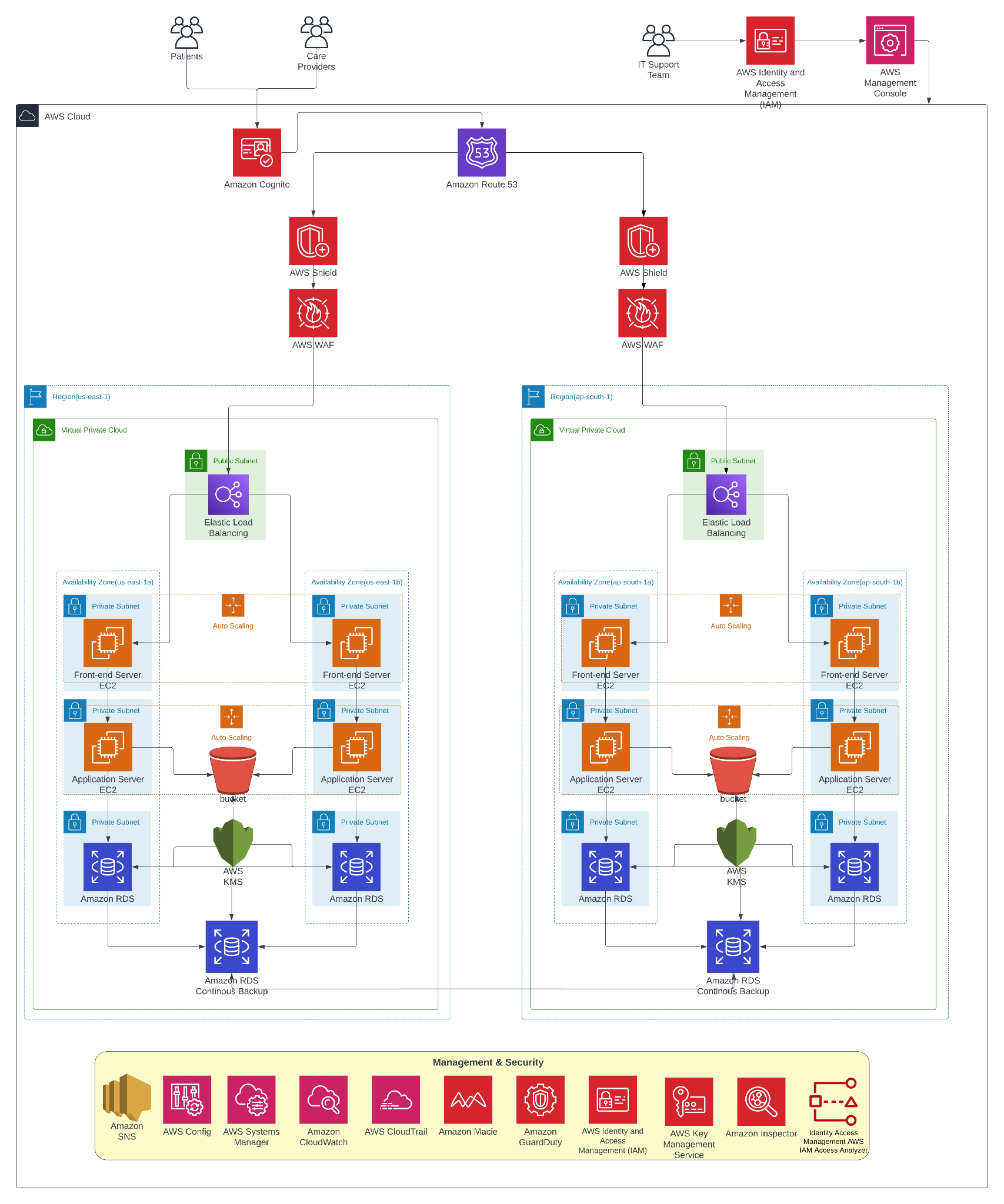
1. **EC2 Instance Auto Scaling and Deletion Protection Not Enabled Vulnerability**:

* Configuring Auto Scaling for EC2 instances and enabling deletion protection is crucial for both Patients & Care Providers and IT Support. This involves dynamically adjusting capacity based on application demand. Monitoring and adjusting Auto Scaling configurations prevent the accidental loss of instances critical to application performance, ensuring continuous resource availability.

1. **Lack of Disaster Recovery Plan Vulnerability**:

* Developing a comprehensive disaster recovery plan, including failover procedures for critical applications across multiple sites, is essential for both user categories. Regularly evaluating the disaster recovery plan ensures its effectiveness in handling and recovering from unforeseen incidents. This structured approach minimizes downtime and data loss, contributing to robust business continuity.

# **Architecture Diagram**



# **Architecture Details - Patient**

* In this healthcare portal, patients play a very important role in accessing the portal using their devices.
* Patients are involved in performing the following activities:
  + Participate in telemedicine consultation
  + View medical records
  + View test results
  + Schedule appointments
  + Make general inquiries
* To perform or complete any of the activities mentioned above, patients need to log in to the healthcare portal or establish a communication to the portal.
* If patients log in, they are served with a **login portal** that is connected to **Amazon Cognito**.
  + **Amazon Cognito** is a customer identity and access management (**CIAM**) service that we are using instead of AWS IAM roles.
  + The biggest reason for doing this is because **AWS IAM** is foundational for **managing access to AWS resources** while **Amazon Cognito** is specifically for **user authentication and authorization**.
  + This service is **cost-effective** because it scales automatically to accommodate the number of patients and is a fully managed service meaning it is serverless architecture that reduces server maintenance.
  + In the healthcare portal, **Amazon Cognito** provides a secure identity store and federation options such that it can scale to millions of patients.
  + The reason why we utilized Amazon Cognito in place of any other services is that it supports login with **social identity providers, SAML, and OIDC-based identity** **providers**.
  + Since it supports various compliance standards, including **HIPAA**, this becomes the most suitable service to be utilized for the patients to log into the portal.
  + Also, Cognito operates on open identity standards like **OAuth2.0, SAML 2.0, and OpenID Connect** which makes it quite easier to integrate with an extended ecosystem of front-end and back-end development resources without much hassle.
  + Additionally, Cognito **supports MFA**  which adds an extra layer of security.
  + MFA in Amazon Cognito can be enabled for user pools which in our case are the patients.
  + Due to the wide support of **SMS-based and Voice call-based MFA**, these services are employed for the patients to use. This **eliminates** the use of a **separate SNS system** **saving costs**.
  + Also, the **minimum length** for the **username** is set to be 6 characters, and the minimum length for the **password** is set to be 12 characters that must have one compulsory uppercase character, a lowercase character, a number, and a special character using Amazon Cognito service.
* After successful login with Amazon Cognito, patients access the resources through our healthcare portal’s custom domain which is managed by **Amazon Route 53**.
  + We are using it to manage the **DNS records**.
  + We have also associated our healthcare portal’s domain to reach the **Elastic Load Balancer** to perform the intended actions requested by the patient.
* Before the patient’s request is sent to the **Elastic Load Balancer**, the request travels through an **AWS Shield** and **AWS WAF**.
  + We have **enabled DDoS protection** using **AWS Shield** in order to protect against **DDoS attacks**.
  + **AWS Shield** helps to **detect** and **mitigate** malicious traffic, which ensures that legitimate requests from **legitimate patients** are reaching the portal.
  + With the help of **AWS Shield** we are making sure our healthcare portal remains **available** and **responsive**, even during **DDoS attacks**.
  + Later, the request passes through **AWS WAF** from **AWS Shield**.
  + **AWS WAF** operates at the **application layer** and protects our web application from web-based attacks like SQL-I, XSS, etc.
  + In AWS WAF, we have **defined rules and policies** to handle **incoming requests** in order to **identify malicious patterns** in the HTTP requests which would in turn **generate logs** and perform an action like either **blocking the request, allowing it or triggering some actions** as designed.
  + Additionally, we have employed **logging and monitoring** in **AWS WAF**. This would help in **analyzing traffic patterns, security events, and potential threats**.
  + We have implemented **AWS CloudWatch Logs** to **review and analyze these logs**.
  + **AWS WAF** also provides the ability to **continuously monitor and adjust security policies** based on evolving threats on our healthcare portal. **Rules** can be **refined** and **blacklists** can be **updated**.
  + **AWS WAF and AWS Shield** are **region-specific**, therefore, multiple AWS WAF and AWS Shield are put in place.
* After the successful security checks through **AWS Shield** and **AWS WAF**, the request finally hits the Elastic Load Balancing through the designated Region out of the two Regions via the VPC for the activity that the patient has requested or has intended to perform.
* Through the Elastic Load Balancing, the request moves further into the cloud and hits the respective Front-end and Application Servers based on the allotment by the load balancer moving into the least loaded Availability Zone of the two Availability Zones in each of the two Regions.
* In the event that there is a sudden increase or decrease of patients accessing the Healthcare portal, the resources Auto-Scale based on the number of patients.
* The data that the patients provide or request is encrypted using the AWS Key Management Service (AWS KMS). Both the data at rest and in transit are encrypted using AWS KMS.
* Moreover, **Amazon Macie** is employed to **discover, identify, and classify sensitive data**. It uses **Machine Learning Algorithms** to detect the **PII** automatically irrespective of whether the data is being **structured** or not. **Amazon Macie** also helps with **HIPAA** compliance requirements. This helps in securing patient data.
* Here, a **three-tier architecture** network design is followed.
  + The **Front-end Server, Application Server, RDS, and S3 buckets** are placed in the **Private Subnet**. This allows us to **isolate** the **backend systems** from the patients who would never need direct access to these resources.
  + **Elastic Load Balancing** is placed in a **Public Subnet**. This allows us to handle incoming client requests and the load balancer forwards these requests to the backend servers in the private subnet. Hence, keeping the **backend infrastructure hidden** from direct access.
* The Healthcare Portal access is designed in such a way that each patient individually is given **access** to only their medical records. Since Amazon **Cognito** has the ability to generate **unique user accounts, unique patient IDs** can be generated and used to assign **access control**.
* All the patients are added to a group defined by the **policies** and **roles** considering the unique patient IDs such that patients have **no more or less access** to any other resources other than their **own medical records, test results, make general inquiries and schedule appointments.**

# **Architecture Details - Care Provider**

* In this healthcare portal, **Care Providers** play a very important role in accessing the portal.
* **Care Providers** include:
  + Doctors
  + Nurses
  + Specialists
  + Administrative Staff
  + Pharmacists
* **Care Providers** are involved in performing the following activities:
  + Diagnosing and treating patients
  + Accessing patients’ Medical Records
  + Prescribing medications, and overseeing their care plans
  + Provide expertise in specific medical fields
  + Collaborating with other care providers (third-party) like insurance companies, hospitals, medical specialists, etc
  + Appointment scheduling
  + Billing
  + Administrative functions supporting patient care
* To perform or complete any of the activities mentioned above, **Healthcare Providers** need to **log in** to the healthcare portal or **establish a communication** to the portal.
* While **Healthcare Providers** log in, they are served with a **login portal** that is connected to **Amazon Cognito**.
  + **Amazon Cognito** is a customer identity and access management (**CIAM**) service that we are using instead of AWS IAM roles.
  + The biggest reason for doing this is because **AWS IAM** is foundational for **managing access to AWS resources** while **Amazon Cognito** is specifically for **user authentication and authorization**.
  + This service is **cost-effective** because it scales automatically to accommodate the number of healthcare providers and is a fully managed service meaning it is serverless architecture that reduces server maintenance.
  + In the healthcare portal, **Amazon Cognito** provides a secure identity store and federation options such that it can scale to millions of healthcare providers.
  + The reason why we utilized Amazon Cognito in place of any other services is that it supports login with **social identity providers, SAML, and OIDC-based identity** **providers**.
  + Since it supports various compliance standards, including **HIPAA**, this becomes the most suitable service to be utilized for the healthcare providers to log into the portal.
  + Also, Cognito operates on open identity standards like **OAuth2.0, SAML 2.0, and OpenID Connect** which makes it quite easier to integrate with an extended ecosystem of front-end and back-end development resources without much hassle.
  + Additionally, Cognito **supports MFA**  which adds an extra layer of security.
  + MFA in Amazon Cognito can be enabled for user pools which in our case are the healthcare providers.
  + Due to the wide support of **SMS-based and Voice call-based MFA**, these services are employed for the healthcare providers to use. This **eliminates** the use of a **separate SNS system** **saving costs**.
  + Also, the **minimum length** for the **username** is set to be 6 characters, and the minimum length for the **password** is set to be 12 characters that must have one compulsory uppercase character, a lowercase character, a number, and a special character using Amazon Cognito service.
* After successful login with Amazon Cognito, patients access the resources through our healthcare portal’s custom domain which is managed by **Amazon Route 53**.
  + We are using it to manage the **DNS records**.
  + We have also associated our healthcare portal’s domain to reach the **Elastic Load Balancer** to perform the intended actions requested by the patient.
* Before the patient’s request is sent to the **Elastic Load Balancer**, the request travels through an **AWS Shield** and **AWS WAF**.
  + We have **enabled DDoS protection** using **AWS Shield** in order to protect against **DDoS attacks**.
  + **AWS Shield** helps to **detect** and **mitigate** malicious traffic, which ensures that legitimate requests from **legitimate patients** are reaching the portal.
  + With the help of **AWS Shield** we are making sure our healthcare portal remains **available** and **responsive**, even during **DDoS attacks**.
  + Later, the request passes through **AWS WAF** from **AWS Shield**.
  + **AWS WAF** operates at the **application layer** and protects our web application from web-based attacks like SQL-I, XSS, etc.
  + In AWS WAF, we have **defined rules and policies** to handle **incoming requests** in order to **identify malicious patterns** in the HTTP requests which would in turn **generate logs** and perform an action like either **blocking the request, allowing it or triggering some actions** as designed.
  + Additionally, we have employed **logging and monitoring** in **AWS WAF**. This would help in **analyzing traffic patterns, security events, and potential threats**.
  + We have implemented **AWS CloudWatch Logs** to **review and analyze these logs**.
  + **AWS WAF** also provides the ability to **continuously monitor and adjust security policies** based on evolving threats on our healthcare portal. **Rules** can be **refined** and **blacklists** can be **updated**.
  + **AWS WAF and AWS Shield** are **region-specific**, therefore, multiple AWS WAF and AWS Shield are put in place.
* After the successful security checks through **AWS Shield** and **AWS WAF**, the request finally hits the **Elastic Load Balancing** through the designated **Region** out of the **two Regions** via the **VPC** for the activity that the patient has requested or has intended to perform.
* Through the Elastic Load Balancing, the request moves further into the cloud and hits the respective **Front-end and Application Servers** based on the allotment by the load balancer moving into the least loaded **Availability Zone** of the **two Availability Zones** in each of the **two Regions**.
* In the event that there is a sudden increase or decrease of care providers accessing the Healthcare portal, the resources Auto-Scale based on the number of care providers.
* The data that the care providers provide or request is encrypted using the **AWS Key Management Service** (**AWS KMS**). Both the **data at rest and in transit** are **encrypted** using **AWS KMS**. Also, since Patients' records use **AWS KMS**, these can be securely accessed by the Care Providers.
* Moreover, **Amazon Macie** is employed to **discover, identify, and classify sensitive data**. It uses **Machine Learning Algorithms** to detect the **PII** automatically irrespective of whether the data is being **structured** or not. **Amazon Macie** also helps with **HIPAA** compliance requirements. This helps in securing not only patient data but also the data of care providers.
* Here, a **three-tier architecture** network design is followed.
  + The **Front-end Server, Application Server, RDS, and S3 buckets** are placed in the **Private Subnet**. This allows us to **isolate** the **backend systems** from the patients who would never need direct access to these resources.
  + **Elastic Load Balancing** is placed in a **Public Subnet**. This allows us to handle incoming client requests and the load balancer forwards these requests to the backend servers in the private subnet. Hence, keeping the **backend infrastructure hidden** from direct access.
* **Care Providers** are **not** provided with **IAM access**. Since Amazon **Cognito** has the ability to generate **unique user accounts**, **unique care provider IDs** can be generated and used to assign **access control**.
* The Healthcare Portal access is designed in such a way that each care provider individually is given access to only the resources they need access to using **Amazon Cognito**:
  + Patients’ Medical Records - Doctors, Specialists
  + Medications, and Care Plans - Doctors, Nurses, Specialists, Pharmacists
  + Send and receive messages with other care providers (third-party) like insurance companies, hospitals, medical specialists, etc - Doctors, Administrative Staff
  + Appointment Directory - Doctors, Specialists
  + Billing - Administrative Staff
* All the care providers are added to a **group** defined by the **policies** and **roles** considering the unique care provider IDs such that care providers have **no more or less access** to any other resources other than those described above.
* We also have incorporated **Amazon Simple Notification Service (SNS)** in order for the care providers to communicate with third parties like insurance companies, hospitals, and medical specialists.
  + **Amazon SNS** is a completely managed messaging service that enables communication of messages or notifications allowing care providers to efficiently communicate with **third parties** like insurance companies, hospitals, and medical specialists. The following can be achieved using SNS:
    - **Care Providers** might be required to communicate with **insurance companies** for various **Claims Processing, Billing,** and **Reimbursement**.
    - **Care Providers** might be required to communicate with other **Hospitals** for **Patient Transfers, Consultations,** and **Health Information Exchange**.
    - **Care Providers** might be required to communicate with **Medical Specialists** for **Consultations, Referrals,** and **Collaborative Care**.

# 

# **Architecture Details - IT Support**

* The IT support team is the backbone of our Healthcare System. This team plays a critical role in ensuring the smoother operations, security, and reliability of a healthcare system.
* IT Support team consists of:
  + End-User Support Representatives
  + Database Administrators
  + System Administrators
  + Super Admins
* IT Support team is responsible for various aspects like
  + Infrastructure Management
    - AWS Services Configuration
    - AWS Service Interaction
    - Networking and VPC Design
    - Database Configuration
    - Resource Scaling
  + Security Implementation
    - IAM Policies and Access Controls
    - IAM Role Management
    - Security Groups and Network ACLs
    - Encryption Management
    - Security Patching and Updates
  + Monitoring and Incident Response
    - CloudWatch Setup
    - CloudTrail Setup
    - Incident Response
    - Performance Monitoring
  + Backup and Disaster Recovery
    - AWS Backup Implementation
    - Disaster Recovery Planning
  + Continuous Improvement
    - Cost Optimization
    - Performance Optimization
  + Training and Documentation
    - Team Training
    - User Training
    - Documentation
* Since there are further sub-teams and a wider range of activities that the IT Support Team performs, we will be delving deeper into them describing the components.
* **AWS Identity and Access Management (AWS IAM)**:
  + The IT Support Team logs into their AWS accounts using AWS IAM through their browser.
  + They provide their credentials consisting of **username** of the **minimum length** set to be 6 characters, a **password** with the minimum length set to be **12 characters** that must have one compulsory uppercase character, a lowercase character, a number, and a special character enforced by the **password policy** and an **MFA code** that is configured through **IAM** that can be a **time-based OTP** through a **hardware or software token**.
  + **IAM** has been configured with **policies** that define the **permissions** granted to each user of the IT Support Team. The **policies** have been specified with what **actions** the IT Support Team members can perform on which **AWS resources**.
  + Additionally, **IAM roles** have also been assigned to the IT Support Team members based on their **specific roles** and **responsibilities**.
  + Every user is provided with only the **permissions** that they need. **No extra permissions** have been provided keeping in mind the **policy of least privilege**.
  + On successful completion of the above **authentication**, they are redirected to the **AWS Management Console**.
* **AWS Management Console:**
  + Through the AWS **Management Console**, IT Support Team can interact with all of the **AWS services and resources** available or configured.
  + Again, the **access is limited** based on the **permissions** granted by **IAM**.
  + By interacting with the AWS Management Console, IT Support Team can configure AWS services, manage instances, review logs, and respond to incidents.
  + Through the AWS Management Console we have configured our VPC. This VPC is managed through the AWS Management Console.
  + Using the console, Auto Scaling features and policies are configured for automatically scaling EC2 instances based on the required demand.
  + Furthermore, Amazon RDS, Amazon S3 buckets, Amazon KMS has been configured using this AWS Management Console.
* **Amazon Cognito:**
  + Amazon Cognito is set up by the IT Support Team and utilized by the Patients and Care Providers in the backend for Authentication and Authorization.
  + **Amazon Cognito** is a customer identity and access management (**CIAM**) service that we are using instead of AWS IAM roles for Patients and Care Providers.
  + The biggest reason for doing this is because **AWS IAM** is foundational for **managing access to AWS resources** while **Amazon Cognito** is specifically for **user authentication and authorization**.
  + This service is **cost-effective** because it scales automatically to accommodate the number of Patients and Care Providers and is a fully managed service meaning it is serverless architecture that reduces server maintenance.
  + In the healthcare portal, **Amazon Cognito** provides a secure identity store and federation options such that it can scale to millions of patients and care providers.
  + The reason why we utilized Amazon Cognito in place of any other services is that it supports login with **social identity providers, SAML, and OIDC-based identity** **providers**.
  + Since it supports various compliance standards, including **HIPAA**, this becomes the most suitable service to be utilized for the patients and care providers to log into the portal.
  + Also, Cognito operates on open identity standards like **OAuth2.0, SAML 2.0, and OpenID Connect** which makes it quite easier to integrate with an extended ecosystem of front-end and back-end development resources without much hassle.
  + Additionally, Cognito **supports MFA**  which adds an extra layer of security.
  + MFA in Amazon Cognito can be enabled for user pools which in our case are the patients and care providers.
  + Due to the wide support of **SMS-based and Voice call-based MFA**, these services are employed for the patients and care providers to use. This **eliminates** the use of a **separate SNS system** **saving costs**.
  + Also, the **minimum length** for the **username** is set to be 6 characters, and the minimum length for the **password** is set to be 12 characters that must have one compulsory uppercase character, a lowercase character, a number, and a special character using Amazon Cognito service.
* **Amazon Route 53:**
  + **Amazon Route 53** is set up by the IT Support Team and utilized by the Patients and Care Providers in the backend for accessing the resources through our healthcare portal’s custom domain which is managed by **Amazon Route 53**.
  + Management of **DNS records** is done using Amazon Route 53.
  + We have also associated our healthcare portal’s domain to reach the **Elastic Load Balancer** to perform the intended actions requested by the patients and care providers.
* **AWS Shield and AWS WAF:**
  + AWS Shield and AWS WAF are set up by the IT Support Team. The requests from Patients and Care Providers travel through **AWS Shield** and **AWS WAF** before moving to the **Elastic Load Balancer**.
    - We have **enabled DDoS protection** using **AWS Shield** in order to protect against **DDoS attacks**.
    - **AWS Shield** helps to **detect** and **mitigate** malicious traffic, which ensures that legitimate requests from **legitimate patients** are reaching the portal.
    - With the help of **AWS Shield** we are making sure our healthcare portal remains **available** and **responsive**, even during **DDoS attacks**.
    - Later, the request passes through **AWS WAF** from **AWS Shield**.
    - **AWS WAF** operates at the **application layer** and protects our web application from web-based attacks like SQL-I, XSS, etc.
    - In AWS WAF, we have **defined rules and policies** to handle **incoming requests** in order to **identify malicious patterns** in the HTTP requests which would in turn **generate logs** and perform an action like either **blocking the request, allowing it or triggering some actions** as designed.
    - Additionally, we have employed **logging and monitoring** in **AWS WAF**. This would help in **analyzing traffic patterns, security events, and potential threats**.
    - We have implemented **AWS CloudWatch Logs** to **review and analyze these logs**.
    - **AWS WAF** also provides the ability to **continuously monitor and adjust security policies** based on evolving threats on our healthcare portal. **Rules** can be **refined** and **blacklists** can be **updated**.
    - **AWS WAF and AWS Shield** are **region-specific**, therefore, multiple AWS WAF and AWS Shield are put in place.
  + After the successful security checks through **AWS Shield** and **AWS WAF**, the request finally hits the **Elastic Load Balancing** through the designated **Region** out of the **two Regions** via the **VPC** for the activity that the patients and care providers have requested or have intended to perform.
* **AWS Region:**
  + We have set up **two AWS regions** namely **“us-east-1”** and **“ap-south-1”** that are replicas of each other.
  + The reason for having multiple regions is to add redundancy, fault tolerance, and the capability to withstand regional failures.
  + Use of multiple regions helped to distribute incoming traffic across instances in both regions, ensuring high availability and fault tolerance.
  + Also, **Auto Scaling** has been achieved across both regions to automatically adjust the number of **EC2** instances depending on the demand to handle varying **loads**.
  + **Amazon RDS** and **S3** have been configured for **cross-region** **replication** to maintain a standby database in the secondary region to enable rapid failover and replication for critical S3 buckets to ensure redundancy and availability of healthcare data in both regions in the event of a regional outage or disaster.
  + **CloudWatch** and **CloudTrail** have been configured in both regions for comprehensive **monitoring** and **auditing** allowing the IT Support team to **detect** and **respond** to **incidents** quickly.
  + In the event of a **failover** scenario, critical services will **seamlessly switch** to the **secondary region** in case of a **disaster**.
* **Virtual Private Cloud (VPC):**
  + VPC has been configured and managed using the AWS Management Console.
  + VPC has been divided into multiple subnets. Public and Private subnets have been configured.
  + Public Subnets consist of Elastic Load Balancing while the Private Subnets consist of a Front-end server(EC2), Application Server(EC2), and Amazon RDS.
  + Using VPC, route tables are configured and network ACLs are adjusted.
  + Isolation of services has been achieved using subnets that implement a layer of security isolating the resources from being directly exposed to the public internet.
  + **Security groups** have been configured to control the **inbound** and **outbound traffic** and **unused security groups** are **deleted**.
  + CloudWatch Logs are employed to capture and analyze logs generated by VPC components for monitoring and troubleshooting.
  + Also the VPC Flow Logs have been enabled to capture information about the IP traffic going to and from network interfaces in the VPC.
* **Availability Zone:**
  + The IT Support Team has strategically leveraged Availability Zones (AZs) in each of the two replicated regions to enhance the reliability, fault tolerance, and performance of the healthcare system.
  + Critical resources such as EC2 instances, ELB, and RDS instances have been deployed across multiple Availability Zones to ensure that if one AZ experiences issues, the other AZ can handle the workload, maintaining high availability.
  + Also, Auto Scaling groups have been configured to distribute EC2 instances across multiple AZs, enabling automatic scaling based on demand while maintaining fault tolerance.
  + Availability Zones have been utilized for deploying read replicas of Amazon RDS databases providing redundancy and allowing for load balancing of database read queries. Also, RDS database backups across multiple AZs have been done enhancing data backup and recovery capabilities.
* **Public and Private Subnet:**
  + Public subnets are used to host critical components like ELB requiring direct internet access by patients and care providers.
  + Public subnets have been configured by the IT Support Team to automatically assign public IP addresses to resources, ensuring seamless communication with the internet.
  + Also, Security groups and network ACLs have been defined to control inbound and outbound traffic in order to ensure necessary communication while maintaining security.
  + CloudWatch Logs have been deployed to capture and analyze logs from resources in public subnets to help aid in monitoring.
  + CloudTrail has been enabled in order to audit API calls related to resources in public subnets, enhancing visibility into actions performed on the resources.
  + Private subnets have been designated in order to host EC2 instances and Amazon RDS databases that store sensitive data.
  + Network ACLs have been set up to control traffic at the subnet level which also adds an additional layer of security for resources in private subnets.
  + Implementation of private subnets has created a highly secure environment for the backend processing of sensitive healthcare data, protecting it from direct exposure to the internet.
* **Elastic Load Balancing, Front-end Server(EC2), Application Server(EC2) and Amazon RDS:**
  + We have utilized **three-tier architecture** network design.
  + The **Front-end Server, Application Server, RDS, and S3 buckets** are placed in the **Private Subnet**. This allows us to **isolate** the **backend systems** from the patients who would never need direct access to these resources.
  + **Elastic Load Balancing** is placed in a **Public Subnet**. This allows us to handle incoming client requests and the load balancer forwards these requests to the backend servers in the private subnet. Hence, keeping the **backend infrastructure hidden** from direct access.
  + Front-end Server(EC2) is configured and managed.
  + Application Server(EC2) is configured and managed.
  + Using the Amazon Management Console, Amazon RDS instances are configured and managed. This includes setting up databases, adjusting instance sizes, and managing backups.
  + The IT Support Team makes regular updates and patches the operating systems and software on EC2 instances. This helps in maintaining a secure and up-to-date environment.
  + Security groups associated with EC2 instances are configured by the IT Support to control inbound and outbound traffic. The IT Support Team has defined rules to allow only necessary communication meaning that it has implemented the principle of least privilege for enhanced security.
  + CloudWatch has been deployed to monitor the performance and health of EC2 instances.
* **Amazon RDS Continuous Backup:**
  + The IT Support has defined and managed the data retention period for backups and increased the data retention period.
  + Continuous Backup retains backups for a long specified duration and also provides historical recovery points in order to align with the healthcare system's data retention policies.
  + Also, automated backups have been scheduled without manual intervention.
  + Continuous backups allow point-in-time recovery of the database in the event of data corruption
  + Accidental deletion has been enabled to minimize data loss.
* **Auto Scaling:**
  + Auto Scaling has been configured for both front-end and back-end Amazon EC2 instances in order to ensure that the healthcare system can automatically scale its capacity based on demand. Scalability contributes to security by handling varying workloads without compromising performance.
  + Auto Scaling has been facilitated to manage updates and patching.
  + Also, IAM roles are assigned to EC2 instances launched by Auto Scaling. This ensures that instances have been assigned with the necessary permissions to interact securely with other AWS services and resources.
  + The best part of Auto Scaling is that it regularly performs health checks on instances
* **Amazon S3:**
  + S3 buckets are configured and managed by the AWS Management console.
  + Versioning has been enabled on S3 to track changes to objects over time.
  + Server access logging has been enabled on S3.
  + Bucket policies and access controls have been configured to regulate access to S3 buckets. The IT Support Team has defined granular permissions using IAM roles and policies to ensure that only authorized users can access, modify, or delete data stored in S3.
  + Server side encryption has been implemented in S3.
  + Based on the IAM roles, access to S3 buckets is given and limited.
  + AWS CloudTrail is configured to log S3 API calls and actions.
  + Through the implementation of Macie, it automatically identifies and classifies sensitive healthcare information within S3.
* **Amazon KMS:** 
  + The data that the care providers provide or request is encrypted using the **AWS Key Management Service** (**AWS KMS**). Both the **data at rest and in transit** are **encrypted** using **AWS KMS**. Also, since Patients' records use **AWS KMS**, these can be securely accessed by the Care Providers and Patients.
  + Through the AWS Management console, AWS Key Management Service (KMS) is configured and managed.
  + Through KMS, key creation, rotation, and managing permissions for encrypted resources is possible.
* **Amazon SNS:**
  + The IT Support team has also incorporated **Amazon Simple Notification Service (SNS)** in order for the care providers to communicate with third parties like insurance companies, hospitals, and medical specialists.
  + **Amazon SNS** is a completely managed messaging service that enables communication of messages or notifications allowing care providers to efficiently communicate with **third parties** like insurance companies, hospitals, and medical specialists. The following can be achieved using SNS:
    - **Care Providers** might be required to communicate with **insurance companies** for various **Claims Processing, Billing,** and **Reimbursement**.
    - **Care Providers** might be required to communicate with other **Hospitals** for **Patient Transfers, Consultations,** and **Health Information Exchange**.
    - **Care Providers** might be required to communicate with **Medical Specialists** for **Consultations, Referrals,** and **Collaborative Care**.
* **AWS Config:**
  + Through AWS Config, the IT Support team continuously monitors the configuration settings of AWS resources within the healthcare system, including EC2 instances, S3 buckets, RDS databases, and other critical components.
  + It also helps the IT Support Team to configure rules to perform automated compliance checks against predefined security standards and best practices.
  + AWS Config has been configured to generate alerts and notifications in order to detect non-compliant configurations or changes that may pose a security risk.
  + AWS Config has been integrated with AWS CloudTrail to provide a comprehensive view of API events and changes made to resources.
  + The IT Support Team has configured AWS Config to retain historical configuration data for a specified period.
* **AWS Systems Manager:**
  + AWS Systems Manager allows centralization of data from multiple AWS services and automates tasks across AWS resources. We can group resources, like Amazon EC2 instances, Amazon S3 buckets, and Amazon RDS instances, allowing us to manage them collectively for easier administration.
  + It helps to automatically apply patches, configure across instances, enforce compliance, and manage system security. With Systems Manager, we can maintain system security and compliance by scanning instances against the patch, configuration, and custom policies.
* **Amazon CloudWatch and AWS CloudTrail:**
  + We have implemented **AWS CloudWatch Logs** to **review and analyze these logs**.
  + Any failed authentication attempts will be monitored and logged through AWS CloudTrail and Amazon CloudWatch.
  + Through CloudTrail logs, KMS keys can be tracked and monitored.
  + AWS CloudTrail has been integrated with AWS Config to provide a comprehensive view of API events and changes made to resources.
  + CloudWatch has been deployed to monitor the performance and health of EC2 instances.
  + **CloudWatch** and **CloudTrail** have been configured in both regions for comprehensive **monitoring** and **auditing** allowing the IT Support team to **detect** and **respond** to **incidents** quickly.
  + AWS CloudTrail is configured to log S3 API calls and actions.
* **Amazon Macie:**
  + **Amazon Macie** is employed to **discover, identify, and classify sensitive data**. It uses **Machine Learning Algorithms** to detect the **PII** automatically irrespective of whether the data is being **structured** or not. **Amazon Macie** also helps with **HIPAA** compliance requirements. This helps in securing not only patient data but also the data of care providers.
  + Macie automatically identifies and classifies sensitive healthcare information within S3.
* **Amazon GuardDuty:**
  + Amazon GuardDuty helps to continuously analyze logs and network activity within the healthcare system to detect malicious and unauthorized behavior.
  + GuardDuty coverage across multiple AWS accounts and regions has been implemented to monitor all relevant accounts and regions to ensure comprehensive threat detection for the healthcare system's distributed architecture.
  + GuardDuty has been configured to automatically generate findings and take remediation actions.
  + GuardDuty generates security findings based on identified threats and then the IT Support Team can review these findings and prioritize responses based on the potential impact on security.
  + It is integrated with CloudWatch Events and SNS in order to provide real-time alerts.
* **Amazon Inspector:**
  + Amazon Inspector is utilized to perform automated vulnerability assessments on Amazon EC2 instances within the healthcare system. It identifies security vulnerabilities in the operating system, libraries, and application packages.
  + Inspector evaluates instances against security best practices and benchmarks.
  + Amazon Inspector has been integrated with CloudWatch Events to provide notifications when assessment runs are completed.
  + Amazon Inspector provides detailed reports on assessment findings, including identified vulnerabilities and security best practice violations to the IT Support Team.
  + IT Support initiates regularly scheduling Inspector assessments to establish a continuous monitoring mechanism for identifying and addressing security vulnerabilities. This proactive approach contributes to maintaining a secure environment.
* **IAM Access Analyzer:**
  + AWS Access Analyzer helps identify resources in the AWS environment such as Amazon S3 buckets, IAM roles, AWS KMS keys, AWS Lambda functions etc. It does this by analyzing permissions granted using policies and reports whether any policies allow access from outside the AWS account or organization.
  + When Access Analyzer detects a resource that is shared with an external resource, it generates a finding. Users can review these findings to determine whether the access is intended and safe or if actions need to be taken to revise the permissions for better security. This is crucial for maintaining least privilege access and ensuring that only the necessary permissions are granted.
* **Disaster Recovery Plan:**
  + The IT Support team has configured Amazon RDS instances for continuous backup to capture changes to the database in real-time.
  + Also, they have leveraged automated snapshots for point-in-time recovery.
  + They have also enabled versioning for the S3 buckets storing critical healthcare data to track and recover from accidental deletions or modifications.
  + Cross-region replication has been implemented for Amazon RDS databases to ensure data resilience in the event of a regional outage.
  + AWS KMS keys have been set to replicate across regions to ensure encrypted data can be accessed and decrypted in the event of a disaster.
  + We have Implemented regular key rotation for AWS KMS to enhance security and compliance.
  + We will be Conducting regular disaster recovery drills to validate the effectiveness of the recovery plan.
  + In case of a regional outage, failover to the replicated Amazon RDS instance in another region.
  + Traffic has been routed to the S3 bucket in the secondary region.
  + Regular training sessions will be conducted on the latest recovery procedures.
  + By implementing this disaster recovery and backup plan, the healthcare system can ensure data integrity, availability, and rapid recovery in the face of unforeseen incidents.

# 

# **References**

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/AccessAnalyzer/findings.html>

<https://aws.amazon.com/iam/>

<https://aws.amazon.com/guardduty/>

<https://aws.amazon.com/waf/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/KMS/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/VPC/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/CloudTrail/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/CloudWatchLogs/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/CloudWatch/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/GuardDuty/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/Backup/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/RDS/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/ACM/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/EFS/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/SSM/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/SecretsManager/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/Config/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/Shield/>

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/WAF/>

<https://aws.amazon.com/cognito/details/>

[ENPM665-Group6-Midterm](https://docs.google.com/document/u/0/d/1dgFrcYNWNYcQW7jqtPe7Ngx_aTu-Zw7kZd5cIn069dw/edit)