ENPM665: Cloud Security
Final Exam: Healthcare company securities vulnerabilities
Instructor: Professor Everett Daviage
Group15: Pradyumna Upadhyay, Sai Preetham Dasari, Ushasri Bhogaraju
Term: Fall '23

Executive Summary

Introduction: A Healthcare company is a critical service provider that handles sensitive data and is subject to regulatory compliance besides being responsible for patient and other stakeholder needs. Therefore, the primary concerns that need to be addressed while migrating their service infrastructure to the Cloud environment, are high availability, data and network security, and implementation of regulatory compliance, besides minimizing operating costs. AWS is a competitive cloud service provider that has the required depth and detail of services required by the company. Therefore, our assessment and recommendations are based on the AWS platform. The proposed secure architecture can be implemented on another cloud service provider if desired by the company. By enabling services such as AWS IAM, AWS Security Hub, AWS Config, AWS Inspector, AWS WAF, AWS Cloud Watch, and AWS Cloud Trail on the proposed cloud formation templates, and by using reports from third-party tools such as Prowler, we were able to get exhaustive reports for analysis. We grouped the vulnerabilities we found under 1. Vulnerability assessment, 2. Data security Assessment, 3. Virtual Machine Vulnerability Assessment, 4. Network security assessment and 5. Disaster Recovery Assessment. A total of 42 vulnerabilities were identified and segregated into critical, high risk, medium risk, and low risk based on their impact on company assets on the cloud, and company data security and compliance requirements. For each of these vulnerabilities, we propose a mitigation plan either by enabling different options under services from within the AWS framework.

Key findings: Our vulnerability assessment was performed around the 5 assessment perspectives listed in the introduction. The key vulnerabilities found under each of these assessment categories are:

1. Vulnerability assessment: We found that existing data protection measures were inadequate. Users/roles/policies are envisaged with the ability for unrestricted access and manipulation of Data. We found that the present data encryption measures were inadequate and that there was no provision for role-based access to things like EC2 instances, which increases the risk due to the compromise of credentials.
2. Data security assessment: We found that there is no real-time monitoring mechanism for enabling logging and alerts. We could not find an automated backup arrangement for RDS instances. We found only one EC2 instance in the infrastructure indicating that no snapshots are being taken periodically. Data is not encrypted either at rest or in transit.
3. Virtual Machine assessment: We found that the VM could be accessed easily as the authentication and authorization requirements are not strong. The EC2 instance access is

set to 0.0.0.0/0 opening it to all IP addresses on the internet making the entire architecture vulnerable to attacks.

4. Network security assessment: We found that the infrastructure is envisaged in a single region without implementing network segmentation. We could not find any Web application firewalls to protect company applications from outside attacks.
5. Disaster Recovery: We could not find a disaster recovery and business continuity plan, identifying actions to be taken by team members in case of disaster. We did not find an arrangement for an alternative site. We found that there was no protection mechanism against deletion for the Cloud formation templates. There were also no backup arrangements for data to be used when restoring the cloud services.

Risk Assessment: Risk assessment was performed by enabling tools and services within the AWS environment and also applying third-party tools such as Prowler. The reports are available here. A risk assessment summary is provided in the report. To summarize, we find that the cloud infrastructure of the Healthcare company in its current form is easy prey to attacks from outside of the cloud infrastructure as well as from data losses due to lack of encryption and insecure access controls from within.

Regulatory Compliance: The following elements of regulatory compliance have been identified and incorporated into our recommendations:

- HIPAA compliance by ensuring logging and restricting access to sensitive patient information to users of the cloud service infrastructure based on their specific needs
- HITECH Act compliance by ensuring EHRs are well protected, manipulated, and accessed only by users/roles with clearance
- Data sharing between hospitals in different geographies following compliance with local laws.

Amazon web services provides Amazon Healthlake, a service that can be used by the company for help in aggregating, organizing and analyzing health data while ensuring security and compliance with the above regulatory requirements.

Recommendations with mitigation plan: We have identified and categorized individual risks to the company cloud infrastructure from a general vulnerability assessment perspective and specific perspectives such as Data security, Virtual Machine, Network, and Disaster recovery. Our recommendations come with an architectural diagram of the proposed infrastructure and mitigation tools for each risk we identified. The risks and tools are detailed under the 'Technical overview' section of this report. The link to the architectural diagram is here. The majority of the resources and services we recommend may be found within the AWS environment.

Conclusion: With the implementation of proposed enablers for monitoring, access control, data, and network security of the cloud infrastructure, the company can operate securely and efficiently in the cloud environment.

1. Proposed Architectural Diagram

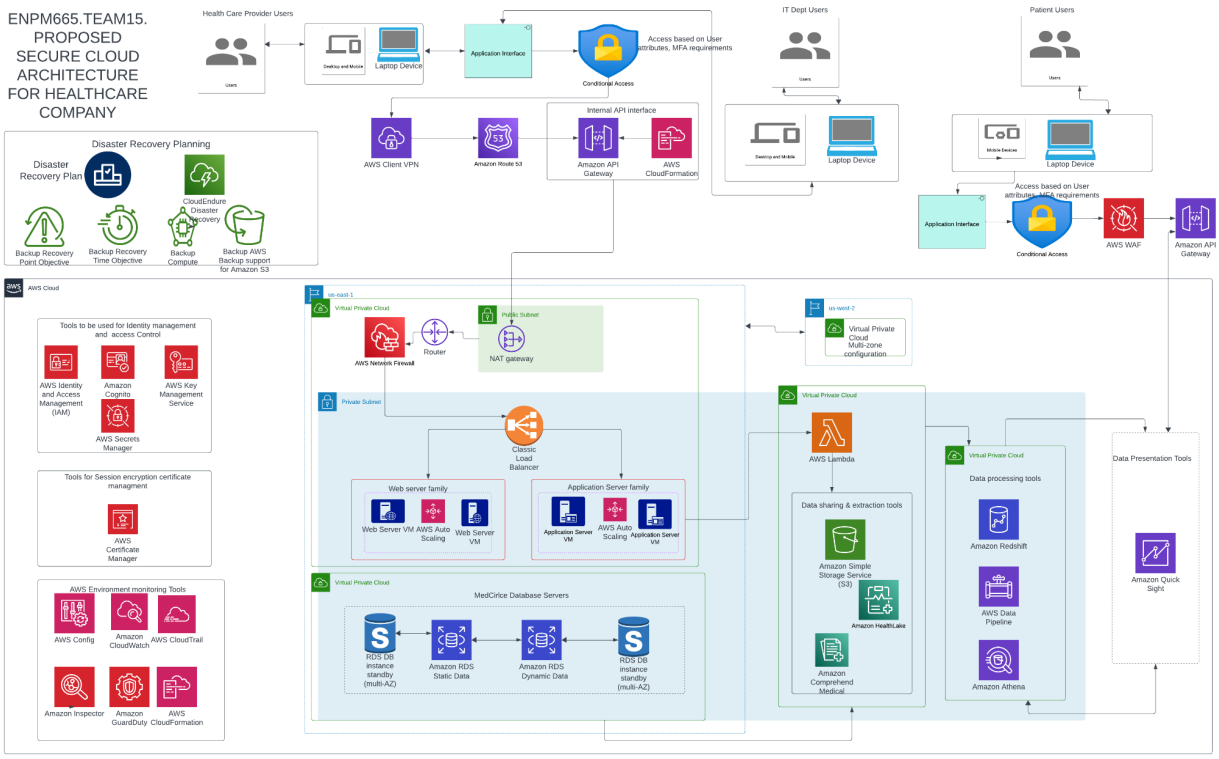


Figure: Architecture diagram proposed for healthcare application

Scenario 1: Patient's Perspective

The patients making use of the healthcare application should be able to access their medical records at all times due to the sensitive nature of the records themselves. When designing the infrastructure for such a system, care should be taken to ensure that the system is highly available and there are measures in place to restrict the access of all patients to their medical records.

The patients will only interact with the healthcare application using **HTTPS on port 443**. The usage of HTTPS ensures that the traffic between the patient and the healthcare application is always encrypted. **Amazon Certificate Manager (ACM)** facilitates the use of HTTPS for the healthcare application. ACM issues and manages SSL/TLS certificates required to enable secure communication. These certificates serve as digital credentials that authenticate the identity of the healthcare application's server to the patient's browser.

Before accessing their data on the healthcare application, all patients would need to authenticate themselves using their credentials. We also recommend the use of multi-factor authentication to improve the security of the application and mitigate some of the risks associated with leaked

credentials. **Amazon Cognito** is a fully managed identity and access management service within AWS that provides a simple and scalable way to handle user identities and authentication. We recommend the use of Amazon Cognito as it would allow secure authentication of the users. It has a host of useful features such as username/password authentication, multi-factor authentication, account recovery, and customizable authentication workflows.

All requests by the patients would also first pass through the **AWS Web Application Firewall (WAF)**. The WAF helps safeguard the application against common web attacks such as SQL Injection and Cross-site scripting. Custom rules can also be created in Amazon WAF to address the unique threats or vulnerabilities specific to the healthcare application. Using a WAF greatly increases the security, availability, and reliability of the healthcare application.

The **Amazon API Gateway** serves as the front door for the requests to the healthcare application. It provides a single entry point for patients to access the backend services and data through their requests. Amazon API Gateway can be integrated with Amazon Cognito for user authentication. It can also be integrated with a WAF to provide a defense-in-depth approach. The auto-scaling feature of the Amazon API Gateway also allows the application to handle varying levels of traffic efficiently. The request throttling and caching features of the Amazon API Gateway also help mitigate and handle Denial of Service (DOS) attacks on the application. The API Gateway then propagates the user's request to the back-end of the healthcare application. Based on the user's request, the application logic may access different cloud resources such as AWS S3 buckets, RDS instances, etc. The resulting response may be presented back to the user after undergoing processing and transformation in AWS services such as **Amazon Athena, Amazon Redshift, and AWS Data Pipeline** as required by the application logic. **AWS Quick Sight** can be used to present the response to the user in a clear, concise, and visually appealing manner.

Scenario 2: Care Provider's Perspective

The Care providers have overarching responsibility over all aspects of running the Healthcare company. However, for this analysis, we have maintained focus on a few key aspects of the care provider's responsibilities.

1. Providing access to authorized personnel to cloud resources, through robust authentication and authorization procedures to perform their functions efficiently using suitable AWS services
2. Enabling suitable AWS services for restricting access to bonafide users, monitoring access granted, logging actions performed on resources, automated encrypted Key management, and maintaining secrecy of passwords and other secret information
3. Enabling AWS services to ensure Backups are automated
4. Enabling AWS services and gateways that check inbound and outbound traffic to ensure secure sharing of Data over the network with third parties

5. Disaster Recovery Planning

Key Components of the architecture:

1. Devices to access the application interface by the care provider users: Desktops, Mobile devices, Laptops
2. Application Interface: How the care provider users will interact with the cloud resources of the company
3. VPNs: Used to provide a secure and encrypted connection over the internet to the private network hosting the cloud infrastructure of the Healthcare company
4. DNS resolvers: An instrument to resolve the Domain name input by the care provider user and convert it into a corresponding IP address of the resource
5. API Gateways: This gateway receives the care provider user's API request, enforces security policies, and passes them to the back-end service requested by the user.
6. VPC: A logically isolated section of the cloud environment of the Healthcare company, where different resources to be accessed by the care provider users are launched.
7. Public subnets: Healthcare cloud resources in this space will have IP addresses that allow direct communication with the internet. Inspection and restriction will be enforced through the NAT gateway.
8. Network Firewall: This software application will ensure the separation of resources in the public subnet and the private subnet of the Healthcare company
9. Private subnets: This logical space will hold the Web servers and application servers of the Healthcare company.
10. RDS instances: Database instances of the database engine used by the Healthcare company. The company can use multiple engines such as My SQL, PostgreSQL, MariaDB, and have multiple RDS instances for each of these engines.
11. EC2 instances: The virtual machines spun up by the Healthcare company IT team that will run applications and workloads
12. S3 Buckets : The simple storage space that will hold company documents, sensitive patient data, images, application backups, and log files.
13. Data analysis and reporting tools: The tools required by patients, care providers, and developers for drawing insights and generating required reports
14. Data pipeline tools: For generation of data required by the care providers by performing Data extraction on S3 buckets, query on RDS databases, and run custom scripts on EC2 instances.
15. Monitoring and Flow logs: This is an important aspect of compliance and will be achieved by enabling CloudTrail service (discussed in greater detail in Section 2)
16. Disaster recovery Planning, Disaster recovery plan document with alternate site details, communication plan, team members contact numbers will be put in place and all the staff members will be aware of this document and its contents.

Data flow from the Care Provider's View:

We have envisaged 5 chief types of care provider users of the Cloud resources of the Health care company such as 1. Admin Users, which will include Super Admins, admin support staff, HR, Finance and Billing department users, 2. Doctors, 3. Nurses, 4. Pharmacists and 5. Pathlab users. Each of these users will have individual user based access. They will also be part of user groups. These users and user groups are to be created using AWS IAM service (Section 2.3). Suitable Group policies available under AWS IAM Policies list may be attached to these user groups to enable them to perform their functions on the cloud resources. If more fine grained policies are required, custom policies can be created under the same menu. Further, we propose the creation of some roles that will grant temporary access to sensitive resources such as patient information records so that, where necessary, a user from a different user group can assume the role to perform the necessary action. An admin staff can get read access to patient test results for example, by assuming a role of a 'lab_dept_user'with a read only permissions policy attached to the role.

System access to all the care provider users is envisaged with Desktops, Laptops and Mobile devices, using an application interface. Authentication is user attribute based or role based. The user / role must meet the strong authentication requirements that have been pre configured using AWS IAM service (Section 2.3). In this service discussed more elaborately under Services and methodologies (Section 2.3), Usernames can be created, updated, and deleted. In the present architecture, for DB users, the minimum username length required is 1.

```
Parameters:
  DBName:
    Default: MedCircleDB
    Description: MySQL database
    Type: String
    MinLength: '1'
    MaxLength: '64'
    AllowedPattern: '[a-zA-Z][a-zA-Z0-9]*'
    ConstraintDescription: Must begin with a letter and contain only alphanumeric characters.
```

This can be updated to more complex requirements using the IAM service. Complexity of passwords can be enforced through IAM password management. Using the same service, MFA enabling can be done for users/roles. After authentication, the user is allowed secure access to the AWS Virtual Private Network (Section 2.12) . Here, Amazon Route 53 service (Section 2.16) resolves the client DNS and access to the public subnet is granted through Amazon API gateway. The NAT Gateway is envisaged in the public subnet, providing restriction of inbound traffic and for handling outbound traffic subject to rules from private subnet. Then the user is allowed access through the AWS Network Firewall (Section 2.15) -which inspects incoming and outgoing traffic based on rules and takes appropriate action - to the data and resources such as Web servers and application servers located in the private subnet.

Security: In the dataflow, network segmentation is enforced through separation of resources in the public and private subnets. Dataflow between these resources is monitored through an AWS firewall (Section 2.14) that checks data flows with pre configured rules and allows only compliant data flows. AWS certificate manager (Section 2.13) will ensure provisioning and management of SSL/TLS certificates to ensure session encryption during data transfer to third parties.

In the diagram, we have projected access control to sensitive data through authentication using AWS IAM service (Sec 2.3) module. AWS Secrets Manager service (Sec 2.11) is recommended for safekeeping of API keys, passwords and Database credentials pertaining to the IAM users and roles in the cloud infrastructure. AWS Key management service (Sec 2.8) is recommended to manage data encryption keys. This service can be integrated with S3 Buckets, RDS instances, EBS volumes and Lambda. Using AWS CloudWatch service, (Sec 2.20) alarms may be created for important events such as repeated login failures, indicating possible attempts for unauthorized access.

Compliance: In the diagram, configuring AWS CloudTrail (Sec 2.19) for logging AWS account activity to create event history and logs for compliance auditing is envisaged. AWS config service will be enabled, which will provide a detailed description of changes made to resource configurations, using which detection of unauthorized actions can be detected.

Scenario 3: IT Support Perspective

Scenario:

The cloud infrastructure of the healthcare organization is managed and maintained in large part by the IT department. This covers duties the following:

- Cloud resource provisioning and management (VMs, databases, etc.)
- Installing and upgrading software
- Keeping an eye on and debugging systems
- Making sure that security and adherence are met.

Key Components of the architecture:

- Internet Gateway: The point of entrance into the cloud infrastructure for outside traffic.
- Load Balancers: Traffic should be split among site servers.
- Web Servers: Take care of user requests and host the front end of the website.
- Application Servers: Manage user requests and business logic.
- Database Servers: Save private medical information.
- Cloud Storage: Holds enormous datasets, such as medical pictures.
- Security Tools: Analyze and Monitor security events.
- IAM: To control user access to cloud resources, IAM policies and access controls are employed. The cloud resources of the healthcare organization are only accessible to authorized users.

- VPC: The virtual private cloud (VPC) separates the cloud resources of the healthcare organization from the public cloud and the internet. This aids in defending against intrusions and illegal access.
- Subnet: To further split the cloud resources of the healthcare organization and implement more precise access controls, the VPC is partitioned into subnets.
- Network Access Control Lists (ACLs): Traffic between subnets and the internet is managed by ACLs. The VPC only allows authorized traffic to enter and exit.
- Security Groups: Via security groups, traffic between the virtual machines (VMs) inside the VPC is managed. Only protocols and ports that have been approved can be open.
- Web Application Firewall (WAF): The web servers of the healthcare organization are shielded from common assaults like SQL injection and cross-site scripting by the WAF.
- Data encryption: Every bit of private medical information is secured both in transit and at rest. In the event of a breach or attack, this aids in data protection.
- IT Support Access: Access points specifically designated for IT staff.

Data Flow from IT Support View:

- When a request is made by the IT Support team, the data flow in the healthcare application architecture travels a secure route through several components.
- User Request: Via their device, IT support person requests access to the online application hosted on AWS.
- Access and Authentication: When a request passes via conditional access controls, multi-factor authentication could be necessary in order to confirm the user's identity before allowing access.
- VPN and Network Routing: The user is then safely connected to the application's network within the Amazon VPC by means of AWS Client VPN after the authenticated request has been sent through it.
- Load Balancing: The request is processed by the classic load balancer within the Amazon VPC, which then effectively distributes the network traffic to the web server family within the public subnet.
- Web Server Processing: One of the EC2 instances in the web server family's Auto Scaling group handles the request. This group's automatic scaling of the number of instances up or down allows it to adapt to changing loads.
- Application Server Processing: After then, business logic is carried out by the web server in communication with the application server family within the private subnet. Auto Scaling is another technique used by the application server family to control availability and performance.
- Database Interaction: The application server communicates with the database servers in order to retrieve or save data in response to requests. Whereas Amazon DynamoDB handles requests for dynamic data, Amazon RDS handles queries for structured data. High availability is guaranteed by the multi-AZ deployment configuration of both databases.

- Data Processing: The request may use AWS Lambda functions for serverless computation for specific tasks, including reporting or data analysis, or it may use AWS Data Pipeline to transfer data to Amazon Redshift for sophisticated queries.
- Data Storage and Retrieval: Depending on the demands of the application's data handling and design, data may be saved in or retrieved from Amazon S3 or EFS during this procedure.
- Response to User: The response is delivered back to the user's laptop device via the network once the data has been processed and the required actions have been finished.

2. List of Tools

2.1. Amazon Inspector -This is an AWS service that focuses on identifying vulnerabilities within applications and EC2 instances in a cloud infrastructure. It assesses the security posture of EC2 instances, including the OS, applications, and network configurations in them. It conducts automated security assessments, is scalable and adaptable to large infrastructures. Above all, it prioritizes vulnerabilities according to severity enabling immediate reduction of risk.

Usage: In the Healthcare company infrastructure, we have identified this tool to mitigate the vulnerability we found in VM assessment where in, there was no real-time monitoring configured for safeguarding EC2 instances. Therefore, we have incorporated this tool in the architecture diagram as an enabler for real-time monitoring of EC2 instances.

2.2. AWS Config - AWS config is identified in this architecture for its ability to continuously monitor and capture changes to configurations of important resources. It can provide compliance status of different resources by evaluating them with pre-configured rules. It helps the company ensure compliance with organizational policies, industry standards and security best practices.

Usage: The Healthcare company functions in a multi-user environment. It is important to monitor changes to resource configurations, to immediately identify unauthorized changes. For example, if configuration changes to EC2 instances are left unmonitored, the changes made to the instance may make it an easy target for attack from outside the cloud account. In the case of sensitive data handlers like Healthcare providers, this may mean data breaches, data loss and loss of reputation. Also, to stay competitive, the Healthcare company must follow industry best practices in Data security and compliance at a low cost. AWS config is a service available within the AWS environment which can be enabled and configured to integrate with different resources like EC2 instances, S3 buckets, CloudTrail trails, CloudWatch alarms and many others, for monitoring changes to configurations of these resources. This helps in preventing security risks and ensuring resource compliance with audit requirements at a low cost.

2.3. AWS IAM - This is a powerful AWS service that helps the company manage users, user groups, roles, and permissions to these entities. This service can be used to enforce username requirements, password complexities and manage Multi-Factor authentication requirements. It is the central hub with which the company can match users to resources they need to complete their functions. Most importantly access restrictions to sensitive data can be enforced using AWS IAM service policies. The service provides a long list of AWS managed policies that can be attached to users / groups / roles to manage their access requirements and facilitates creation of custom policies to reflect special permissions.

Usage: While performing vulnerability and VM assessment, we found that the company had weak authentication requirements to access resources. The username and password complexity were not robust enough to protect the company from dictionary attacks or brute force attacks. The policies attached to users such as S3user were overly permissive as also the policies envisaged for admin and developer roles were identical and did not distinguish the access requirements to resources for these roles. We, therefore, identified this service in the architecture to ensure data security, enforce user attribute based and role-based restrictions in access to resources.

2.4. Amazon Athena - Amazon Athena is a fully managed serverless service from the Amazon umbrella of services, that can be integrated with services like Amazon QuickSight to create dashboards and reports based on the results of Athena queries. Athena supports standard SQL and can be used to query data from S3 Buckets without the need for complex ETL processes or data movement.

Usage: In the Healthcare provider architecture, all types of users will need a resource that can read data from various file formats and generate various types of reports in various other formats as per the requirements of the end user. Athena supports this functionality. Since Athena can be integrated with AWS IAM, the company can control access to the service through IAM roles and policies.

2.5. Amazon QuickSight - Amazon QuickSight is a business intelligence tool that helps users quickly visualize and analyze data, create interactive dashboards and share insights with stakeholders, other organizations such as regulatory agencies or vendors. It can integrate with various data sources such as Amazon RDS, Amazon S3 and Amazon Athena.

Usage: We have identified this tool for use by non-technical users such as Doctor's, Admin users, nurses and patients in the cloud architecture. They can not only access data and reports easily but also create dynamic dashboards with data integration.

2.6. AWS CloudEndure & Disaster Recovery - Effective Disaster recovery planning involves a variety of actions. Besides having a comprehensive plan with backup locations, communication planning, creating awareness in teams, identifying an alternative site and ensuring business continuity, coordination becomes a challenge. We therefore recommend the use of CloudEndure, a complete disaster recovery solution from AWS for

this purpose.

Usage: In the existing infrastructure, we did not find suitable arrangements for Disaster recovery and Business continuity. There were no regular backups to recover data from or an arrangement for an alternate site in case of disaster. So, in the absence of any initiative for disaster recovery and business continuity, we recommend AWS CloudEndure to the Healthcare provider, which is a company that provides end to end solutions for disaster recovery.

2.7. Amazon Healthlake - Amazon Healthlake is an AWS service tailored to suit the needs of healthcare service providers. It is a HIPAA compliant service, specially designed to provide a secure and compliant platform to manage health data by healthcare and life sciences organizations. It follows a data lake architecture that enables it to store vast amounts of structured and unstructured data in a central repository. Access can be controlled using AWS IAM service as it can be integrated with all AWS services. It helps data aggregation from different sources such as Electronic Health Records, medical imaging, genomics and other health related data types and provides the core strength required for a healthcare provider.

Usage: To stay competitive and also to provide critical care efficiently, the healthcare provider requires such a service as the Amazon Healthlake to enable users such as Doctors, nurses, pathologists and pharmacists, to store, access and evaluate data from different formats using a unified platform. This service is cost-effective and scalable.

2.8. KMS - Encryption of data in transit and data at rest is a crucial element of any company's security posture. But just encryption of the data is often not adequate. Given the large amount of data companies deal with along with the different categories under which this data can be classified, the number of keys required to encrypt and decrypt the data is often quite high. Management of these keys is equally critical to the company's security posture as the encryption of data itself.

AWS Key Management Service (KMS) is a fully managed service provided by AWS that enables its users to easily create and control the cryptographic keys used to encrypt their data. AWS KMS is designed to make it simple for users to integrate encryption and decryption operations into their applications, ensuring the security of your sensitive information stored in various AWS services and applications.

Usage: AWS KMS is a crucial cog in our proposed infrastructure. The patient data within the healthcare application is highly sensitive. AWS KMS will be used to generate and manage the encryption keys for encrypting the health records. The keys that are used to encrypt the data (Data Encryption Keys) will themselves be encrypted by a master key that is managed by KMS. KMS will also be used for performing key rotation following security best practices to help mitigate the risks associated with long-term key usage.

2.9. Amazon Comprehend Medical - Amazon Comprehend Medical is a natural language processing (NLP) service provided by AWS. It is designed to extract relevant medical

information from unstructured text, such as clinical notes, prescriptions, and medical records.

Usage: Using this service as part of our infrastructure would provide immense value to the healthcare providers using the healthcare application. The service aids in quickly extracting critical information from patient records, helping doctors and nurses make more informed decisions during patient consultations or treatments. An accurate diagnosis based on the extracted information will also greatly benefit all the patients who are treated by the healthcare providers. This service also enhances patient experience by providing a more comprehensible and structured view of their medical history.

2.10. GuardDuty - Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious activity and unauthorized behavior in an AWS environment. It analyzes various data sources, such as VPC Flow Logs, CloudTrail event logs, and DNS logs, to identify potential security threats. The usage of Amazon Guard Duty helps in the detection of and response to security threats in real-time.

Usage: In our proposed infrastructure, Amazon GuardDuty enables the IT Support team to proactively respond to threats, therefore minimizing the impact on the healthcare application and ensuring the continuous availability of critical services. Amazon GuardDuty also helps the application infrastructure meet the requirements set by compliance frameworks such as PCI DSS.

2.11. AWS Secrets Manager - A healthcare application consists of many different databases as well as APIs that are used by different types of users for different kinds of access. Access to these databases and APIs should be controlled using credentials, API keys, and other secrets.

Usage: AWS Secrets Manager is a service that is used to securely store and manage sensitive information such as API keys, database credentials, and other secrets. It provides automatic rotation of the secrets, thereby reducing the risk of unauthorized access. This automatic rotation of secrets greatly reduces the workload of IT Support teams as they no longer need to manually handle the rotation and distribution of credentials, leading to increased operational efficiency. Also, since the process is automated, the risks associated with human error are eliminated greatly. AWS Secrets Manager also integrates seamlessly with a wide range of AWS services, simplifying the management of credentials used by different components of the healthcare application infrastructure.

2.12. AWS Client VPN - AWS client VPN enables secure remote access to AWS resources on the cloud. It provides integration with AWS IAM services for access control and offers support for VPN protocols. It allows configuration of IP address ranges. It follows security best practices, encrypts data in transit and adheres to industry compliance standards making it a robust solution for secure and flexible remote access to AWS cloud resources from a range of devices.

Usage: In the existing infrastructure of the Healthcare company, we did not find encryption for data in transit. Also, users are expected to login to the AWS cloud account from different devices using different IP addresses. Therefore, we recommend enabling AWS client VPN service which is a fully managed service in the AWS environment that can work with AWS IAM to verify user credentials and check for blacklisted IP addresses before allowing access to the network. It also provides encryption of data in transit, which is a crucial requirement for the Healthcare company as sensitive data sharing securely with other hospitals is one of the requirements of the company. Also, the VPN endpoints can be deployed in multiple availability zones to ensure high availability and logging events are sent to AWS CloudWatch for monitoring.

2.13. Certificate Manager - Cloud customers need unexpired SSL/TLS certificates to manage their data transfers over the internet. AWS certificate manager simplifies the process of securing, managing, and using these SSL/TLS certificates for secure communication over the internet by the cloud company.
Usage: In the existing infrastructure of the Healthcare company, we did not find session encryption. One of the reasons could be an expired SSL/TLS certificate. In a Healthcare company, secure data transfer over the internet is a necessity because all its own users and third parties will transact with cloud resources of the company over the internet. ACM provides automated certificate management and removes the need for manual intervention to maintain valid certificates for session encryption. This service also integrates seamlessly with other AWS resources, enabling secure interaction and data transfer over the internet for all these resources.

2.14. Web Application Firewall - All requests by the patients and healthcare providers need to pass through a Web Application Firewall before being processed by the back-end of the application. The WAF protects the health case web application from common web exploits and attacks such as SQL Injection, Cross Site Request Forgery (CSRF), and cross-site scripting.
Usage: AWS WAF can also be set up to perform rate limiting i.e. controlling the number of requests from a particular IP Address. Leveraging such an AWS service can help application developers concentrate on ensuring a better experience for the users rather than worrying about implementing such features from scratch. AWS WAF can also be integrated with a host of other AWS services. For example, integrating AWS WAF with AWS CloudWatch can ensure real-time analysis and response to cyber-attacks.

2.15. Network Firewall - A network firewall is a type of security system that uses pre-established security rules to monitor and manage all incoming and outgoing network traffic. It filters traffic to stop unwanted access and any dangers, serving as a barrier between a trusted internal network and an untrusted external network.
Usage: Applied Network Firewall at Network's Edge and used to filter and manage

incoming and outgoing traffic at the network gateway, shielding the internal network of the healthcare system from harmful assaults and illegal access.

2.16. Route 53 - Amazon Route 53 is a highly available and scalable DNS web service provided by AWS. It employs widely distributed DNS servers to route end-user queries to specific infrastructure, such as web applications, and translates domain names into IP addresses.
Usage: In our system, it ensures that staff and patients may access the website and online services of the healthcare system by converting domain names into IP addresses.

2.17. RedShift - A fully managed data warehousing solution, Amazon Redshift makes it possible to efficiently query and analyze enormous amounts of data. By utilizing parallel query execution and column-like storage technology, it provides quick query performance and scalability.
Usage: In the data warehouse, redshift enables data-driven insights to enhance patient care and spot trends by storing and analyzing vast amounts of patient data.

2.18. Amazon Data Pipeline - With the help of the web service Amazon Data Pipeline, customers can automate the transfer and processing of data between different AWS services and on-premises settings. It facilitates tasks like scheduling, data translation, and transfer.
Usage: In the same VPC as Amazon Redshift, Amazon Data Pipeline guarantees effective data management by automating the transfer and processing of patient data across several AWS services.

2.19. Cloud Trail - An account's activity and API calls are tracked by AWS CloudTrail, a service that offers a history of actions made by users, services, or resources. It makes it possible to audit the AWS infrastructure for governance, compliance, operational risk, and risk management.
Usage: All API calls made to AWS resources are logged, making it easier to comply with laws like HIPAA and making troubleshooting and security incident identification easier.

2.20. Cloud Watch - Real-time monitoring of AWS applications and resources is provided by Amazon CloudWatch, a monitoring and management service. It creates alarms, gathers, and monitors metrics, and reacts automatically to changes in AWS resources.
Usage: With the collection, analysis, and setting of alerts for any problems or performance bottlenecks, CloudWatch can be used to monitor the operation of servers, databases, and apps, among other components of the healthcare system.

2.21. Cloud Formation - AWS CloudFormation is a service that makes use of templates to facilitate the provisioning and management of AWS resources. It makes it possible to create and update a stack—a group of connected AWS resources—in a controlled and predictable way.

Usage: The infrastructure of the healthcare system may be created and managed as code using CloudFormation, which defines resource configuration and guarantees reproducibility and consistency across various settings.

3. Risk Assessment

Sec. & S.No	*Description of Risk*	*Risk label*	*Categorization of Risk under*	*Critical Business functions affected by the vulnerability*
1.1	MFA: Not found for any users in the infrastructure	*Critical*	Vulnerability Assessment, Virtual Machine vulnerability Assessment, Data security Assessment	Health information management, Admin functions, Patient Care, Database security, EHR security, HIE security,
1.2	IAM roles: Envisaged with Overly Permissive policies	*Critical*	Vulnerability Assessment, Data Security Assessment,	Health information management, Admin functions, Patient Care, Database security, EHR security, HIE security,
1.3	IAM roles: No role assigned to any EC2 instance	*High*	Vulnerability Assessment, Network security Assessment	Database management, Application development
1.4	Root volume: Not encrypted	*Critical*	Vulnerability Assessment, Data security Assessment	Health Information Management, PHI protection,
1.5	RDS: Not encrypted	*Medium*	Vulnerability Assessment, Data security Assessment	Health Information Management, Patient Care, Clinical services
1.6	S3 bucket: KMS key encryption not enabled	*High*	Vulnerability Assessment, Data security Assessment	Database, Clinical Services, Health information management
1.7	IMDSv2: Is set as optional in the EC2 instance	*High*	Vulnerability Assessment, Data security Assessment	Database, Clinical Services, Health information management
2.1	IAM policies: Overly permissive, include full read/write access	*Critical*	Data Security Assessment, Vulnerability Assessment	Health information management, Admin functions, Patient Care, Database security, EHR security, HIE security.

2.2	MedCircle Database: No Regular Backup arrangement	*High*	Data Security Assessment, Vulnerability Assessment, Disaster Recovery assessment	Health information management, Admin functions, Patient Care
2.3	Multi-region strategy: Not implemented	*Critical*	Data Security Assessment, Disaster Recovery Assessment	Clinical services, Patient care
2.4	S3 Bucket versioning: Not turned on	*Critical*	Data Security Assessment, Disaster Recovery Assessment	Health information management, Admin functions, Patient Care.
2.5	S3 Bucket: Only have default encryption	*High*	Data Security Assessment, Vulnerability Assessment	Health information management, Clinical services, Admin functions, Patient Care.
2.6	S3 Bucket: Object lock not enabled	*Medium*	Data Security Assessment	PHI data security,Health information management.
2.7	S3 Bucket: Server access logging disabled	*Medium*	Data Security Assessment	Compliance, Health information management
2.8	S3 Bucket: Allows cleartext communication	*Medium*	Data Security Assessment	Health information management, Compliance
2.9	S3 Bucket: Bucket access logging not enabled	*High*	Data Security Assessment	Health information management, Compliance
2.10	EC2 instances: No implementation of automatic snapshot creation at regular intervals	*High*	Data Security Assessment, Disaster Recovery assessment	Patient Care, Clinical Services
2.11	Security events: No real-time monitoring mechanism in place	*High*	Data Security Assessment, Network security assessment	Patient Care, Clinical Services
2.12	RDS instance: No monitoring mechanism	*High*	Data Security Assessment, vulnerability assessment	Patient Care, Clinical Services

	in place			
2.13	RDS database: No failover mechanism envisaged	*Critical*	Data Security Assessment, Disaster recovery assessment	Patient Care, Clinical Services
2.14	RDS instance: Data encryption in transit and at rest not implemented	*High*	Data Security Assessment	Patient Care, Clinical Services
3.1	VM: Weak authentication requirements	*High*	Virtual Machine Vulnerability Assessment, Vulnerability Assessment	Patient Care, Clinical Services
3.2	VM: Database credentials too short	*High*	Virtual Machine Vulnerability Assessment,	Patient Care, Clinical Services
3.3	VM: Inbound and outbound rules source and destination is set to 0.0.0.0/0	*Critical*	Virtual Machine Vulnerability Assessment	Patient Care, Clinical Services
3.4	VM: EBS volumes are not encrypted	*High*	Virtual Machine Vulnerability Assessment	Patient Care, Clinical Services
3.5	VM: Patch management not implemented	*High*	Virtual Machine Vulnerability Assessment	Patient Care, Clinical Services
3.6	VM: Unused security group found	*High*	Virtual Machine Vulnerability Assessment	Patient Care, Clinical Services
3.7	VM: Not using the latest linux version	*High*	Virtual Machine Vulnerability Assessment	Patient Care, Clinical Services
3.8	VM: Missing security patches	*High*	Virtual Machine Vulnerability Assessment	Patient Care, Clinical Services
4.1	VPCs: Multi-region strategy not implemented	*High*	Network security Assessment	Patient Care, Clinical Services

4.2	Network segmentation : Poor	*High*	Network security Assessment	Patient Care, Clinical Services
4.3	Security Group Configuration: Poor	*High*	Network security Assessment	Patient Care, Clinical Services
4.4	Web ACLs: Not found	*High*	Network security Assessment	Patient Care, Clinical Services
4.5	Firewall Policies: Not found	*High*	Network security Assessment	Patient Care, Clinical Services
4.6	Subnet flow logs: Not configured	*High*	Network security Assessment	Patient Care, Clinical Services
4.7	Route 53 resolver DNS firewall rule groups not configured	*High*	Network security Assessment	Patient Care, Clinical Services
5.1	Back-up retention period not enough	*High*	Disaster Recovery Assessment	Patient Care, Clinical Services
5.2	Cloud Formation Template: Termination protection not enabled	*Medium*	Disaster Recovery Assessment	Patient Care, Clinical Services
5.3	RDS instance : Multiple availability zones not configured	*High*	Disaster Recovery Assessment	Patient Care, Clinical Services
5.4	RDS instance: Deletion protection not enabled	*High*	Disaster Recovery Assessment	Patient Care, Clinical Services
5.5	EC2 instance: Auto scaling and deletion protection not enabled	*Medium*	Disaster Recovery Assessment	Patient Care, Clinical Services
5.6	Disaster Recovery plan: Not found	*High*	Disaster Recovery Assessment	Patient Care, Clinical Services, Healthcare management

4. Technical Overview

Health care is a critical service. Therefore the cloud infrastructure must be highly available, secure and failsafe. Healthcare providers are expected to handle sensitive patient health data abiding by local laws, honor data sharing requirements abiding by different laws pertaining to different geographies, and handle payments and credit card processing securely and efficiently. The cloud service infrastructure should be enabled with required monitoring, logging, encryption and access control tools and services that will empower the company in meeting with required regulatory compliances and also run the business safely and efficiently. We were provided with three proposed infrastructure templates for the company. We deployed them in an AWS environment, and analyzed the potential risks it carried by comparing it with recommended standards proposed in the CCSP study guide and AWS recommended best practices, which are available in AWS documentation. We also used industry best practices explored in class lectures to identify risks under the following 5 sections. Besides analyzing the risk and its impact, we have discussed the service or tool available to mitigate the risk.

Section 1: Vulnerability Assessment, vulnerabilities discussion, remediation tool proposed

1.1. MFA: Not found for any users in the infrastructure:

This vulnerability was observed from analyzing Users list from AWS IAM service. Under IAM/Users, there is a column which indicates whether or not MFA is enabled for each user. Enabling MFA reduces risk from unauthorized access. This is especially important for users of privileged accounts having sweeping policies attached to them. ***AWS IAM service*** also provides security recommendations on the IAM Dashboard itself, from where we can proceed to enable MFA for users for which it is not enabled. We can also enable MFA by selecting a user and proceeding to assign an MFA device.

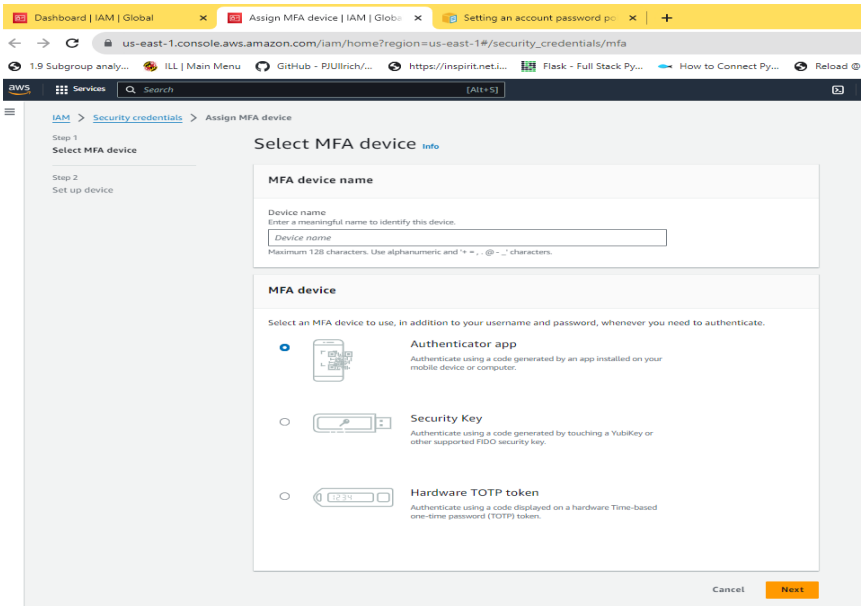


Figure: Enabling MFA for a user, using AWS IAM service

1.2. IAM roles: Envisaged with Overly Permissive policies: IAM roles are envisaged with policies such as IAM policy and Developer policy, that are overly permissive.

They are not created following the principle of least privilege, distinguishing between the different requirements of access to resources, for example between a developer role, an admin role and a user who needs only read only access in the Finance dept. Here is an example of a more restrictive policy suitable for the role of a user in the Finance department. Fine tuning policies to restrict permission to intended resources and no more, can be achieved using the ***AWS Policy Simulator tool.***

Version 4 of AWSBillingReadOnlyAccess

Allows users to view bills on the Billing Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "aws-portal:ViewBilling",
                "billing:GetBillingData",
                "billing:GetBillingDetails",
                "billing:GetBillingNotifications",
                "billing:GetBillingPreferences",
                "billing:GetCredits",
                "billing:GetContractInformation",
                "billing:GetIAMAccessPreference",
                "billing:GetSellerOfRecord",
                "billing:ListBillingViews",
                "ce:ListCostAllocationTags",
                "consolidatedbilling:ListLinkedAccounts",
```

Figure: A restrictive policy with read only access to Billing information for a Finance dept user

Remediation tool/service : AWS IAM/Roles/ Create and attach suitable policy: This menu allows creation of custom policies or selection of AWS managed policies to be attached to a role or a user.

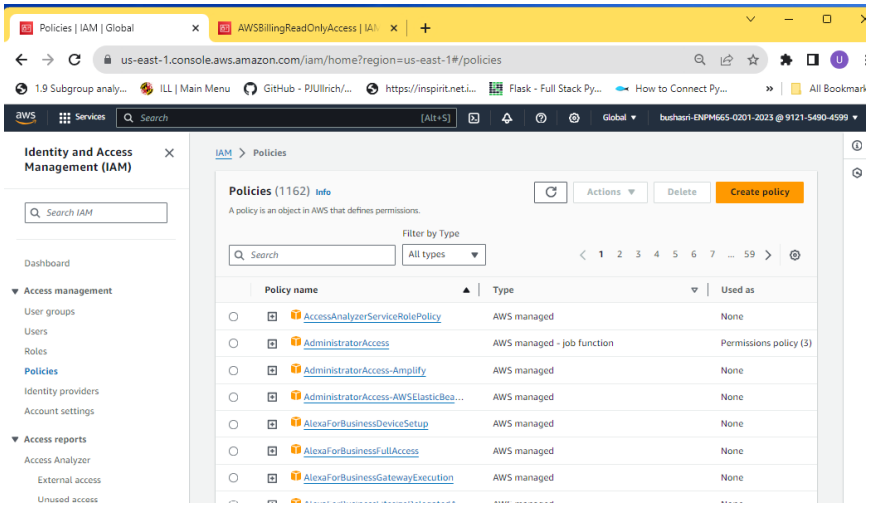


Figure: AWS IAM Policies, create policy menu. Also a number of AWS managed policies to choose from

1.3. IAM roles: No role assigned to any EC2 instance:

In the existing infrastructure, no roles are assigned to things such as EC2 instances. This practice allows secure interaction of the EC2 instances with other AWS services such as S3, RDS etc, without embedding long-term credentials on the instance.

Remediation Tool/Service: AWS IAM service: Under this service, we can create a role under IAM/Roles and attach a suitable policy that reflects access to EC2 instances. There are also AWS managed roles available to choose from. Permit users to assume these roles as required.

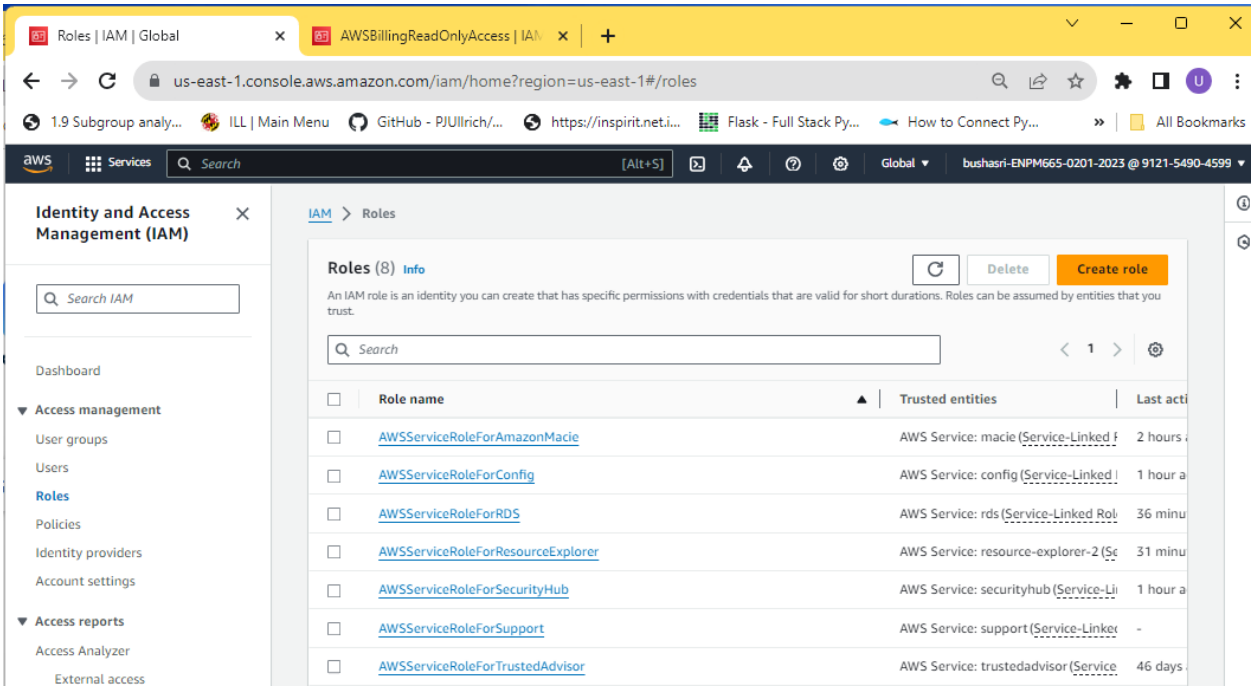


Figure: AWS IAM Roles, create role menu. Also a number of AWS managed roles to choose from

1.4. Root volume: Not encrypted

Root volumes that are not encrypted present a security risk since they can reveal private system configurations or data. Possibility of data breaches or unauthorized access to key system information stored on the root drive.

Remediation Tool/ Service: Make a snapshot of the current, unencrypted volume, duplicate it, and choose encryption settings when copying it to encrypt the root volume. As an alternative, transfer the data from the unencrypted root drive to a new encrypted volume.

1.5. RDS: Not encrypted

The RDS instance's lack of encryption poses a huge security concern, exposing sensitive healthcare data to prospective compromises. Increased risk of data interception or unauthorized access, which could result in compliance violations and jeopardize patient confidentiality.

Remediation Tool/ Service: Using the RDS instance settings in the AWS Management Console, enable encryption for the RDS instance. To activate encryption at rest for the RDS instance, select the relevant encryption option offered by AWS.

1.6. S3 bucket: KMS key encryption not enabled for S3

The KMS key encryption being disabled can have numerous security implications such as data exposure, lack of confidentiality, limited access control, and compliance violations.
Unauthorized access due to a lack of KMS key encryption makes the data stored in the S3 buckets vulnerable. Given that these S3 buckets may contain sensitive medical data of patients,

any information leak could severely damage the reputation of the company and open the company up to potential lawsuits.

Remediation Tool/ Service: Ensuring S3 buckets are encrypted with a customer-managed key in AWS KMS is the first step towards ensuring the confidentiality of patient data in a healthcare application. In addition, the access policies to the KMS Key and S3 buckets should also be appropriately configured by setting up the relevant IAM permissions. The key usage should also be regularly monitored using services such as AWS Cloud Trail and key rotation should also be performed promptly.

1.7. IMDSv2: Is set as optional in the EC2 instance

As IMDS provides important instance metadata and enabling IMDSv2 improves security by guarding against specific kinds of assaults, leaving IMDSv2 (Instance Metadata Service version 2) enabled on an EC2 instance poses a danger to security.

Remediation Tool/ Service: To enforce IMDSv2, update the EC2 instance configuration and set it to mandatory. To change the IMDS settings, use the AWS CLI or AWS Systems Manager. Moreover, use AWS Config and AWS CloudWatch to audit and enforce IMDSv2 usage on a regular basis.

Section 2: Data security Assessment, vulnerabilities discussion, remediation tool proposed

2.1. IAM policies: Overly permissive, include full read/write access, discussed under item 1.2

2.2. MedCircle Database: No Regular Backup arrangement

Important medical data could be lost in the event of a system failure or security compromise if regular backups are not performed. Data loss or corruption makes restoration difficult and jeopardizes the accuracy of patient information and treatment continuity.

Remediation Tool/ Service: To guarantee data resilience and simple recovery, implement a regular backup strategy that includes scheduled backups for the system.

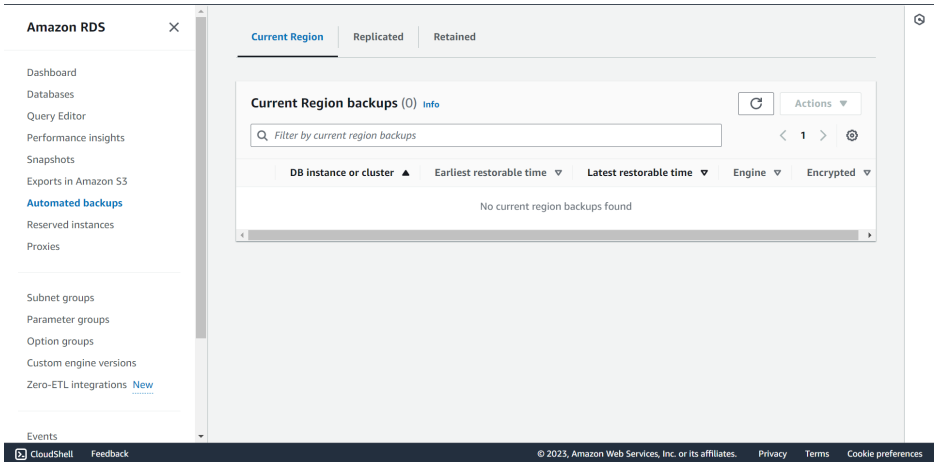


Figure: Create automated backup of AWS RDS for data recovery

2.3. Multi-region strategy : Not implemented

The risk of losing all data during regional outages or disasters is increased when data replication across many locations is lacking. In the event of regional failures, system outages or data unavailability could jeopardize patient care and business continuity.

Remediation Tool/ Service: To provide high availability and catastrophe recovery across geographically dispersed locations, implement a multi-region data replication method.

2.4. S3 Bucket versioning: Not turned on

Configurations of S3 buckets that are vulnerable to flaws leave data open to manipulation, illegal access, and lack of auditability. Inadequate security measures can lead to compromised data integrity, possible breaches, and non-compliance with regulations.

Remediation Tool/ Service: To strengthen data safety and traceability, enable versioning, strong encryption, object locking, access logging, and secure communication protocols in your S3 bucket.

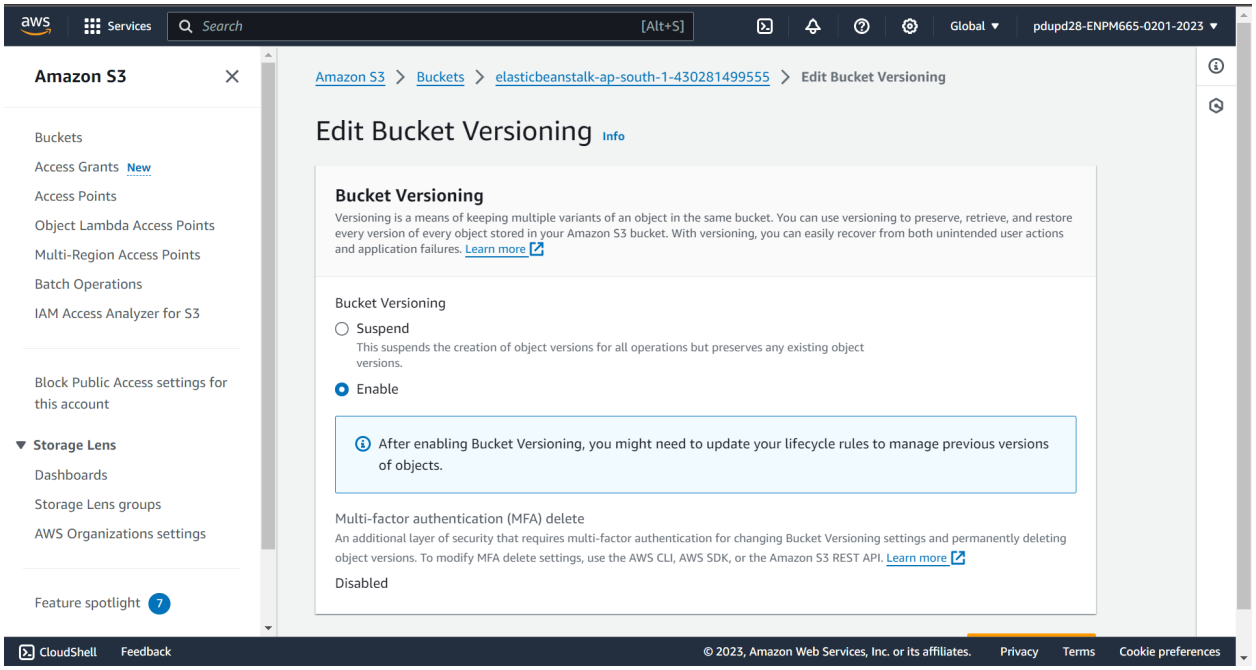


Figure: Bucket Versioning can be enabled under Properties tab of Bucket

2.5. S3 Bucket: Only have default encryption

Inadequate encryption techniques jeopardize patient privacy and breach compliance regulations by exposing private medical data to possible illegal access.

Remediation Tool/ Service: For more robust encryption of S3 bucket data, use AWS Key Management Service (KMS) to manage keys and enable Server-Side Encryption with Customer-Provided Keys (SSE-C).

2.6. S3 Bucket: Object lock not enabled

The lack of object lock capabilities raises the possibility that important healthcare data may be inadvertently altered or maliciously deleted, jeopardizing data security and integrity.

Remediation Tool/ Service: Turn on the Object Lock feature on S3 buckets to stop unauthorized people from changing or erasing important medical data.

2.7. S3 Bucket : Server access logging disabled

Insufficient server access logging makes it more difficult to see changes and attempts to get access, which impedes efforts to do incident response, compliance monitoring, and security analysis.

Remediation Tool/ Service: Turn on S3 Bucket Server Access Logging to monitor and examine changes and requests for access in order to improve security and compliance.

2.8. S3 Bucket: Allows cleartext communication

Enabling cleartext communication puts patient confidentiality at risk, increases the chance of data breaches, and violates privacy laws by exposing healthcare data to interception.

Remediation Tool/ Service: To prevent data eavesdropping, use AWS Certificate Manager to mandate secure communication (HTTPS) for S3 bucket connections and provision SSL/TLS certificates.

2.9. S3 Bucket: Bucket access logging not enabled

The absence of bucket access logging hinders security audits, forensic investigations, and compliance requirements since it prevents visibility into bucket-level access events.

Remediation Tool/ Service: For S3 buckets, enable bucket access logging to track and monitor operations, changes, and access, improving visibility and supporting security audits.

2.10. EC2 instances: No implementation of automatic snapshot creation at regular intervals

In the event of a failure or data corruption, the lack of automated snapshots makes system recovery more difficult, increasing downtime and perhaps resulting in irreversible data loss.

Remediation Tool/ Service: By scheduling and automating snapshots for EC2 instances at regular intervals using AWS Data Lifecycle Manager, you may streamline recovery procedures and lower the risk of data loss.

2.11. Security events: No real-time monitoring mechanism in place

In the absence of real-time monitoring, delayed identification and reaction to security threats may expose users to vulnerabilities for longer periods of time and jeopardize the security of patient data.

Remediation Tool/ Service: For proactive threat prevention and real-time monitoring, use AWS CloudWatch Events. This will allow you to respond quickly to security problems.

2.12. RDS instance: No monitoring mechanism in place

The absence of monitoring for RDS instances puts system stability at risk and may compromise the security and availability of patient data by delaying the early detection of performance problems or security breaches.

Remediation Tool/ Service: Install Amazon CloudWatch to monitor RDS instances continuously, allowing for early problem identification and fixing.

2.13. RDS database: No failover mechanism envisaged

Lack of failover methods raises the possibility of prolonged service outages during RDS instance failures, which could affect the availability and continuity of healthcare services.

Remediation Tool/ Service: To ensure minimal disturbance and continuous availability, deploy Amazon RDS Multi-AZ automatically.

2.14. RDS instance: Data encryption in transit and at rest not implemented

Insufficient data encryption makes healthcare data more susceptible to interception or illegal access, which could result in patient confidentiality and compliance mandate violations.

Remediation Tool/ Service: To provide complete data security for RDS instances, enable encryption using AWS Key Management Service (KMS) for encryption at rest and SSL/TLS for encryption in transit.

Section 3: VM Vulnerability Assessment, vulnerabilities discussion, remediation tool proposed

3.1.VM: Weak authentication requirements

Weak authentication requirements in a cloud infrastructure pose a significant security risk because they make it easier for unauthorized individuals or entities to gain access to sensitive resources and data. Authentication is the process of verifying the identity of users, devices, or services attempting to access a system. Weak authentication practices can lead to several security issues such as unauthorized access, data breaches, identity spoofing, compromised user accounts, and privilege escalation.

Remediation Tool/ Service: Always enable Multi-factor authentication wherever possible. It is a proven way to thwart the vast majority of the attacks mentioned above. Also, enforce strong password policies that include requirements for complexity, length, and regular password changes. Encourage the use of passphrases whenever possible. Most of these measures can be taken in the IAM console in AWS as shown in the image below.

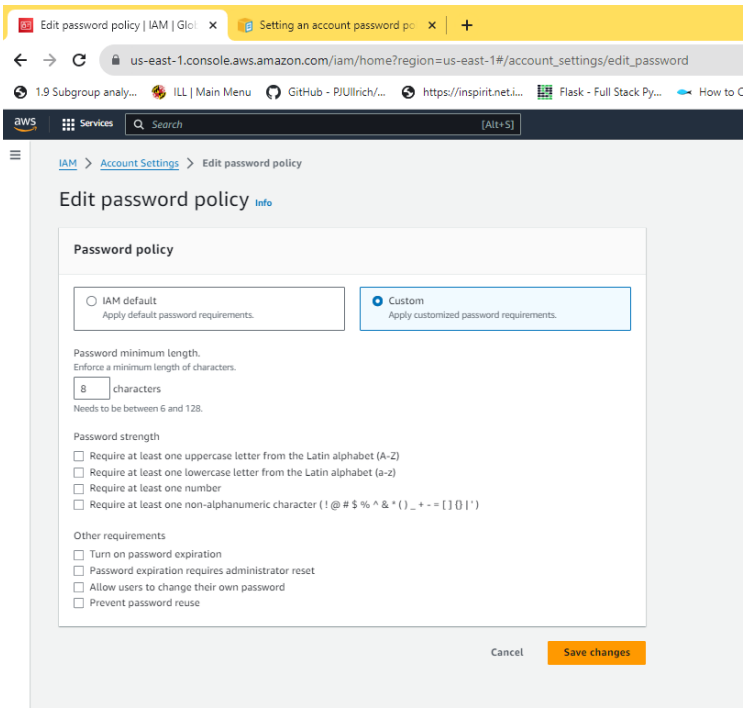


Figure: Password management menu in AWS IAM service

3.2. VM: Database credentials too short

Weak or short database credentials present a security issue because they facilitate brute-force assaults and unapproved access by intruders. Increased vulnerability to possible data breaches, illegal access, and weakened database security.

Remediation Tool/ Service: Update the database credentials with longer, more complicated passwords that adhere to acceptable practices. To securely keep and routinely rotate database credentials, use AWS Secrets Manager.

3.3. VM: Inbound and outbound rules source and destination are set to 0.0.0.0/0

Because it permits unrestricted access, configuring incoming and outbound rules with a source or destination of 0.0.0.0/0 (open to all IP addresses) puts the virtual machine (VM) at risk of unwanted access, attacks, or data breaches.

Remediation Tool/ Service: To limit traffic to particular IP ranges or security groups, and improve network ACL rules and security group rules. Use AWS Config Rules to automate compliance checks by reviewing and updating security group configurations on a regular basis. For centralized security findings and suggestions for safe network configurations, use AWS Security Hub. Additionally, keep an eye on and examine network traffic using AWS VPC Flow Logs to spot any unusual activity.

3.4. VM: EBS volumes are not encrypted

Unauthorized access or security risks could be present for vital healthcare data stored in unencrypted EBS volumes. Unencrypted storage volumes increase the danger of data leakage or breaches.

Remediation Tool/ Service: Create a snapshot of the volume and duplicate it with encryption enabled to encrypt any existing unencrypted EBS volumes. Choose encryption settings for newly created volumes using the AWS Management Console.

3.5. VM: Patch management not implemented

Not implementing patch management for virtual machines (VMs) leaves them vulnerable to known security vulnerabilities that could be exploited by attackers.

Remediation Tool / Service: Implement a robust patch management strategy to regularly update VMs with the latest security patches. Utilize AWS Systems Manager for automated patching and AWS Config for continuous monitoring of VM configurations.

3.6. VM: Unused security group found

The presence of unused security groups poses a security risk as they might inadvertently allow unauthorized access to VMs.

Remediation Tool / Service: Regularly audit and clean up unused security groups. Leverage AWS Config to monitor and enforce security group configurations, and AWS Security Hub for centralized security findings.

3.7. VM: Not using the latest Linux version

Running outdated Linux versions on VMs may expose them to unpatched vulnerabilities and security risks.

Remediation Tool / Service: Regularly update VMs to the latest Linux versions. Use AWS Systems Manager to automate patching, AWS Config for compliance monitoring, and AWS Inspector for vulnerability assessments.

3.8. VM: Missing security patches

Missing security patches on VMs expose them to potential exploitation of known vulnerabilities.

Remediation Tool / Service: Implement a patch management process to regularly update VMs. Use AWS Systems Manager for patch automation, AWS Inspector for vulnerability assessments, and AWS Config for continuous compliance monitoring.

Section 4: Network Security Assessment, vulnerabilities discussion, remediation tool proposed

4.1. VPCs: Multi-region strategy not implemented

Not implementing a multi-region strategy for Virtual Private Clouds (VPCs) can result in a single point of failure and limit the application's availability and resilience.

Remediation Tool / Service: Design and implement a multi-region architecture using AWS Global Accelerator, Route 53 for DNS failover, and AWS CloudFormation for infrastructure as code to ensure high availability across regions.

4.2. Poor Network segmentation

Poor network segmentation exposes the entire network to potential security threats, allowing lateral movement for attackers.

Remediation Tool / Service: Implement strong network segmentation using VPCs, subnets, and security groups. Utilize AWS Network Firewall for advanced threat protection and AWS WAF for web application firewalling.

4.3. Poor Security Group Configuration

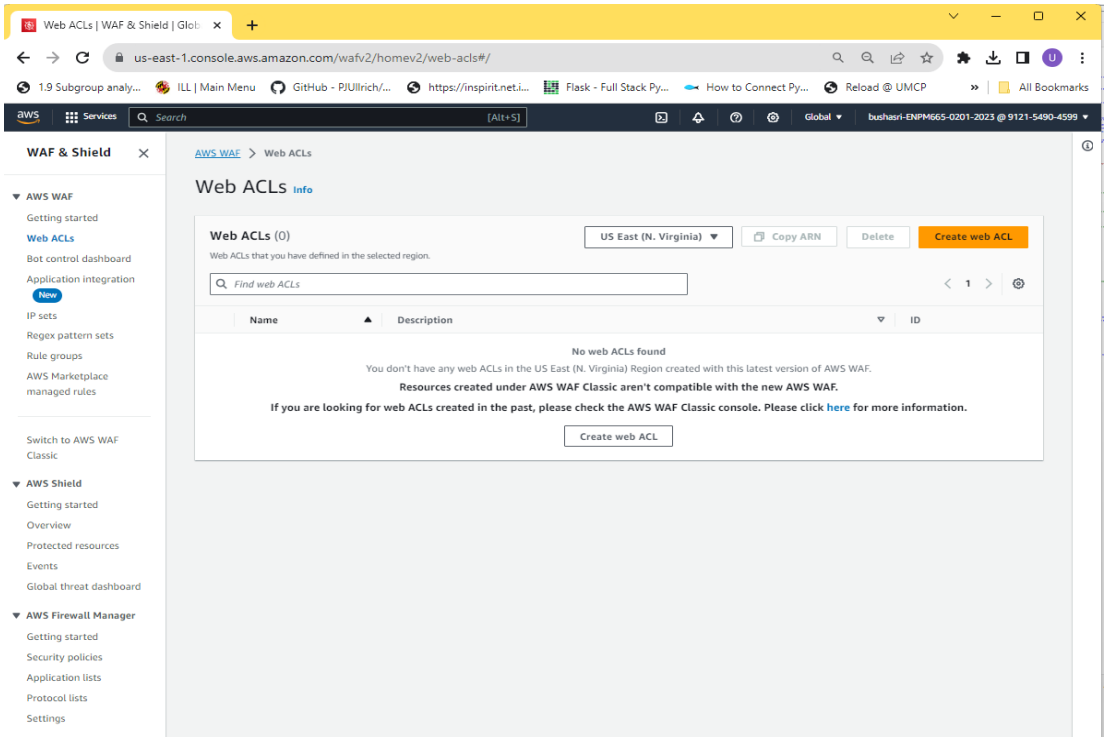
Inadequate security group configurations may result in unintended exposure of services to the internet or overly permissive access.

Remediation Tool / Service: Regularly review and update security group configurations. Use AWS Config Rules for automated compliance checks, and AWS Security Hub for centralized security findings and remediation recommendations.

4.4. Web ACLs not found.

The absence of Web Access Control Lists (Web ACLs) can result in insufficient protection against web-based attacks and malicious traffic, potentially leading to security breaches.

Remediation Tool / Service: Implement Web ACLs using AWS WAF to filter and monitor HTTP/HTTPS traffic. Combine with AWS CloudFront for scalable and secure content delivery, providing an additional layer of protection against web-based threats.



4.5. Firewall Policies not found

The absence of defined firewall policies may leave the infrastructure vulnerable to unauthorized access and cyber threats.

Remediation Tool / Service: Implement and configure firewall policies using AWS WAF for web traffic, AWS Firewall Manager for centralized policy management, and AWS Config for continuous monitoring and compliance checks.

4.6. Subnet flow logs not configured

Flow logs capture information about the IP traffic going to and from network interfaces in different VPCs, providing valuable insights into network traffic patterns, helping with troubleshooting, and enhancing security monitoring.

Without flow logs, the detailed visibility into the network traffic within subnets is missing. Flow logs capture information such as source and destination IP addresses, ports, protocols, and action taken (accepted or rejected), which is crucial for monitoring and analysis.

Remediation Tool/ Service: The subnet flow logs can be configured in the VPC Dashboard of the AWS Management Console. Also ensure that the right IAM roles are configured to grant necessary permissions for publishing flow logs data. Additionally, configure appropriate retention periods for the logs to retain historical data for analysis and compliance purposes.

4.7. Route 53 resolver DNS firewall rule groups not configured

Amazon Route 53 Resolver DNS Firewall provides a way to filter and control the DNS queries and responses that flow through your Resolver endpoints. DNS Firewall rule groups allow the user to define rules for what types of DNS traffic should be allowed or blocked.
Not having the DNS firewall rule groups configured could leave the DNS infrastructure vulnerable to various threats, including malicious domains or unwanted content. This could expose the network to potential security threats, such as DNS-based attacks or unauthorized access to specific domains.

Remediation Tool/ Service: Amazon Route 53 console or AWS Command Line Interface (CLI) should be used to define DNS Firewall rule groups. Within each rule group, rules should be created that define the conditions for allowing or blocking DNS traffic. These rules can be specific to the functioning of the healthcare application and can also be based on threat intelligence feeds.

Section 5: Disaster Recovery Assessment, vulnerabilities discussion, remediation tool proposed

5.1. Back-up retention period not enough

Not having sufficient backup retention policies can lead to the loss of historical data and previous versions of important files. In the event of data corruption, accidental deletions, or system failures, data recovery may become impossible. Many industry regulations and standards also mandate organizations to retain data for a specified period. Failure to comply with these standards can result in legal consequences.
Remediation Tool/ Service: Amazon RDS offsets automated backups and database snapshots. Configuring automated backups with an appropriate retention period ensures that a database can be restored to a specific point in time. Additional services like AWS Backup can also be used for managing backup policies and retention periods.

5.2. Cloud Formation Template: Termination protection not enabled

One of the key issues that was found was the stacks for the healthcare application could be terminated very easily. This could lead to the entire infrastructure being wiped out in the event of an account compromise.

Remediation Tool/ Service: Disable the ‘DeleteStack’ action on all application stacks. Also utilize resource locks, including the ‘aws:cloudformation:delete-stack’ lock type, which can prevent the deletion of specified Cloud Formation stacks. Using Cloud Formation stack policies to control updates to the stack is a good way to provide the stack's protection against termination. Implementing resource locks provides an additional layer of protection against accidental or unauthorized terminations.

5.3. RDS instance: Multiple availability zones not configured

The resilience and high availability of the system are diminished when numerous availability zones are not configured. Vulnerability to service disruptions or outages in the event of an availability zone failure.

Remediation Tool/ Service: To enable Multi-AZ deployment, make changes to the RDS instance settings. By changing the RDS instance settings and choosing the Multi-AZ deployment option, this may be accomplished through the AWS Management Console.

5.4. RDS instance: Deletion protection not enabled

The risk of inadvertent or deliberate deletions rises when RDS instances lack deletion protection. Possible loss of patient or test result data or interruption of service as a result of crucial RDS instances being inadvertently deleted.

Remediation Tool/ Service: For RDS instances, use the AWS Management Console to enable deletion protection. By selecting this option, the RDS instance won't be inadvertently deleted.

5.5. EC2 instance: Auto scaling and deletion protection not enabled

The risk of resource scarcity or unintentional instance termination escalates when auto scaling and deletion protection are absent. Possible interruption of healthcare services because of inadequate resources or unintentional shutdown of crucial EC2 instances.

Remediation Tool/ Service: Using AWS services, create an Auto Scaling Group (ASG) for EC2 instances to implement auto-scaling. Establish scalability policies, minimum and maximum instances, and the desired capacity. To avoid unintentional termination, enable deletion protection for EC2 instances via the AWS Management Console.

5.6. Disaster Recovery plan: Not found.

The importance of a plan that the team can execute incase disaster strikes cannot be overstated. The plan must be communicated, and tested and awareness must be created in employees about the solution. Prior to the development of the plan, a Risk assessment and Business Impact analysis may be done. Important elements of the plan document include

1. Identification of an alternate site and infrastructure to ensure business continuity
2. List of all critical systems and applications with Recovery time objective and Recovery point objective for each of them
3. Defining roles and responsibilities of individuals involved in the recovery process

4. A communication plan outlining how information will be disseminated during and after disaster recovery along with contact details of key persons of the disaster recovery team
5. Definition of backup schedules, and storage locations
6. Testing of the plan and recording the outcomes.

References

[1] AWS Reference Architecture
https://aws.amazon.com/architecture/reference-architecture-diagrams/?solutions-all.sort-by=item.additionalFields.sortDate&solutions-all.sort-order=desc&whitepapers-main.sort-by=item.additionalFields.sortDate&whitepapers-main.sort-order=desc&awsf.whitepapers-tech-category=*all&awsf.whitepapers-industries=*all

[2]. AWS Identity and Access Management
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

[3]. Cloud Endure Disaster Recovery Tool
https://aws.amazon.com/marketplace/search/results?searchTerms=cloudendure+disaster+recovery

[4]. AWS Certificate Manager
https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html

[5] AWS Documentation https://docs.aws.amazon.com/

[6] Certified Cloud Security Professional Official Study Guide - Ben Malisow

[7] ENPM665 Cloud Security Video Lectures