

ENPM665 - Homework 5: Terrapin Health Systems HIPAA Cloud Compliance Audit

Name: Raghava Gatadi

UMD ID: raghavag / 121941190

Course & Section: ENPM665, 0101

Introduction

Terrapin Health Systems is a middle-sized healthcare provider that is transitioning critical and sensitive healthcare-related data, including Protected Health Information (PHI), to the AWS cloud. Any organization that handles PHI is required to be HIPAA (Health Insurance Portability and Accountability Act) compliant. HIPAA requires substantial administrative, physical, and technical safeguards to protect the confidentiality, integrity, and accessibility of PHI. Non-compliance with this act can result in monetary fines, possible legal action, or loss of trust with the public.

The goal of this assignment is to review the organization's AWS cloudformation template using a custom HIPAA focused CIS benchmark checklist. The intent of this review is to document configuration gaps that are a risk to PHI and offer remediations on how to appropriately secure PHI according to applicable regulations and best practices before deployment.

Control Analysis and Checklist

This assessment is solely based on configuration details provided in the AWS cloudFormation template.

| CIS Benchmark Control | Status (Compliant/ Non-Compliant) | Justification |
|---|--|---|
| CIS 2.1.4 - S3 bucket must have Block Public Access Enabled | Non-Compliant | In the PublicAccessBlockConfiguration section, all four fields are set to false. And the S3 policy allows public (principle: “*”) read/write. |
| CIS 2.1.5 - S3 bucket must enforce secure transport (deny non-HTTPS requests) | Non-Compliant | The S3 Bucket policy does not include a deny statement with the AWS:SecureTransport condition set to false. |
| CIS 2.2.1 - RDS instance must have encryption-at-rest enabled | Non-Compliant | In the AssessmentRDSInstance section the field StorageEncrypted is set to false, which should be true to be HIPAA compliant. |
| CIS 2.2.3 - RDS instances must not be publicly accessible | Non-Compliant | In the AssessmentRDSInstance section the field PubliclyAccessed is set to true, which should be set to false, and in the AssessmentRDSSecurityGroup CidrIP is set to 0.0.0.0/0 (meaning publicly accessible). |
| CIS 2.3.1 - EFS file systems must | Non-Compliant | In the AssessmentEFS section the Encrypted |

| | | |
|---|---------------|---|
| be encrypted at rest | | field is set to false, which should be set to true for HIPAA compliance. |
| CIS 3.5 - CloudTrail logs must be encrypted at rest using KMS CMKs | Non-Compliant | The KMSKeyId is not configured on the AWS::CloudTrail::Trail resource. |
| CIS 3.2 - CloudTrail log file validation must be enabled | Non-Compliant | In the properties of AssessmentCloudTrail, the LogValidationEnables field is set to false, which should be true for HIPAA compliance. |
| CIS 5.1.1 - EC2 instance EBS volumes must be encrypted | Non-Compliant | The Encrypted property within the Block DeviceMapping for the EC2 instance is set to false. |
| CIS 5.7 - The EC2 Metadata Service must enforce IMDSv2 only | Non-Compliant | The AssessmentEC2Instance is missing the metadataOptions property, which means by default it uses IMDSv1, which is not HIPAA compliant. |
| CIS 1.16 - IAM policies must not grant full (:) administrative privileges | Non-Compliant | In the AssessmentIAMPolicy section, Action and resources are set to "*" which provides full administrative access. |
| CIS 1.8 / 5.2 - IAM account password policy must meet HIPAA requirement (Minimum 14 Characters) | Non-Compliant | In the AssessmentIAMAaccountPasswordPolicy properties, the MinimumPasswordLength field is set to 8, which should be 14 as per HIPAA compliance rules. |
| CIS 1.9 - IAM password policy must prevent password reuse | Non-Compliant | The AssessmentIAMAaccountPasswordPolicy policy is missing the PasswordReusePrevention property. |
| CIS 1.18 - EC2 instances must be launched with an IAM instance profile | Compliant | The AssessmentEC2Instance references the IAMInstanceProfile (!ref AssessmentInstanceProfile) |
| CIS 3.6 - Customer-managed KMS keys should have key rotation enabled | Non-Compliant | In the AssessmentKMSKey section, the EnableKeyRotation field is set to false, which should be true for HIPAA compliance. |
| CIS 2.1.2 - S3 buckets should have versioning enabled with MFA Delete | Non-Compliant | The AssessmentS3BucketVersioning is explicitly set to suspended. There is no configuration for MFA delete. |
| CIS 3.1 - CloudTrail logging must be enabled | Compliant | The isLogging property for the AssessmentCloudTrail is correctly set to true. |

Risk Analysis

For all non-compliant controls, the risk is a direct violation of HIPAA technical safeguards, primarily concerning unauthorized access, disclosure, and modification of PHI.

| Non-compliant Control | Risk Statement (HIPAA Implication) |
|---|--|
| CIS 2.1.4 / 2.1.5 (S3 Public Access / Secure Transport) | The lack of public access blocks and failure to enforce HTTPS creates a direct path for unauthorized public disclosure and man-in-the-middle attacks on PHI stored in the S3 bucket, leading to a HIPAA data breach. |
| CIS 2.2.1 / 2.3.1 / 5.1.1 (RDS/EFS/EBS Encryption) | Failure to encrypt at rest for databases and file systems means that if the underlying storage is accessed or stolen, PHI is exposed in clear text. This is a direct violation of the HIPAA Encryption standard. |
| CIS 2.2.3 (RDS Publicly Accessible) | Exposing the RDS instance publicly (Publicly Accessible: true and 0.0.0.0/0 ingress) vastly increases the attack surface, enabling potential unauthorized network access to the primary PHI database via brute force or exploitation. |
| CIS 3.5 / 3.2 (CloudTrail KMS Encryption / Validation) | CloudTrail logs are sensitive audit data. Without KMS encryption and log file validation, audit trails of PHI access are susceptible to unauthorized alteration or viewing, compromising the integrity of incident response and forensic evidence. |
| CIS 5.7 (EC2 IMDSv1 allowed) | Allowing IMDSv1 makes the EC2 instance vulnerable to Server-Side Request Forgery (SSRF) attacks, which could allow attackers to steal temporary IAM credentials. These stolen credentials could grant unauthorized access to PHI in other services (like S3 or RDS). |
| CIS 1.16 (IAM Policies: *.* Privileges) | Granting an IAM role full administrative privileges (Action: "*", Resource: "**") violates the principle of Least Privilege. If this role is compromised, an attacker gains total unauthorized control over the entire AWS environment and all PHI within it. |
| CIS 1.8 / 1.9 (IAM Password Policy) | A short minimum password length (8 characters) and failure to prevent password reuse significantly weaken authentication controls. This increases the risk of successful brute-force or credential-stuffing attacks, leading to unauthorized system access and PHI disclosure. |
| CIS 3.6 (KMS Key Rotation Disabled) | Disabled key rotation increases the lifespan of a compromised CMK key material, extending the window during which encrypted PHI is at risk of unauthorized decryption if the key is ever stolen. |
| CIS 2.1.2 (S3 Versioning Suspended) | Suspending S3 versioning eliminates the ability to recover PHI data that is accidentally or maliciously deleted or modified. This compromises the availability and integrity of PHI. |

Recommendations/Improvements

| Non-compliant Control | Actionable Remediation Recommendations |
|---|--|
| CIS 2.1.4 / 2.1.5 (S3 Public Access / Secure Transport) | Set all four BlockPublicAcls, BlockPublicPolicy, IgnorePublicAcls, and RestrictPublicBuckets property values to true. Add a deny statement to the S3BucketPolicy requiring aws:SecureTransport to be true. |
| CIS 2.2.1 / 2.3.1 / 5.1.1 (Data Encryption) | Set Encrypted to true for RDS and EFS resources. Set Encrypted to true for EBS volume mapping for the EC2 Instance. |
| CIS 2.2.3 (RDS Publicly Accessible) | Set Publicly Accessible to false for the RDS instance. Restrict the CidrIp in the AssessmentRDSSecurityGroup to specific VPC CIDR blocks or other private sources, not 0.0.0.0/0. |
| CIS 3.5 / 3.2 (CloudTrail) | Add the KMSKeyID property to the AssessmentCloudTrail and reference the CMK ARM. Set LogFileValidationEnabled to true. |
| CIS 5.7 (EC2 IMDSv1 allowed) | Add the metadataOptions property to the AssessmentEC2Instance with HttpTokens: required to enforce the use of IMDSv2. |
| CIS 1.16 (IAM Policies: *.* Privileges) | Revise the PolicyDocument for AssessmentIAMPolicy to strictly adhere to the Least Privilege principle, replacing Action: "*" and Resource: "*" with only the specific permissions and resources necessary for the EC2 role's function. |
| CIS 1.8 / 1.9 (IAM Password Policy) | Increase minimum password length to 14. Add PasswordReusePrevention and set it to a minimum of 5 (or more). Ensure RequireUppercaseCharacters, RequireLowercaseCharacters, RequireNumbers, and RequireSymbols are set to true. |
| CIS 3.6 (KMS Key Rotation Disabled) | Set EnableKeyRotation to true for the AssessmentKMSKey resource. |
| CIS 2.1.2 (S3 Versioning Suspended) | Set the Status property for AssessmentS3BucketVersioning to Enabled. Implement MFA Delete in a resource policy or using the S3 console once deployed. |

Conclusion and Overall Compliance Posture.

The review of the Terrapin Healthcare systems CloudFormation template reveals a critically non-compliant security posture. Out of the 16 essential controls reviewed, 14 were found non-compliant with HIPAA.

The environment, as currently defined, contains fundamental security flaws that would expose highly sensitive PHI to significant risk of unauthorized access, public disclosure, and integrity compromise. Specific severe issues include:

1. **Public Exposure:** An S3 bucket is publicly accessible, and the core RDS database is publicly exposed to the internet.

2. **Lack of Encryption:** Critical data stores (RDS, EFS, EBS) lack mandatory encryption at rest.
3. **Over-Privilege:** An IAM role has full administrative privileges (Action: "*", Resource: "*"), creating a massive security liability.

Overall Compliance Posture: HIGH-RISK NON-COMPLIANT.

Next Steps: Terrapin Health Systems must not deploy this template. Immediate remediation of all 14 non-compliant controls is required, focusing first on public exposure and encryption gaps, to achieve a compliant security posture before any PHI is migrated to the environment.

Supporting Evidence

1. CIS 2.1.4 / 2.2.3 (Public Exposure)

```
AssessmentS3Bucket:
  Type: AWS::S3::Bucket
  Properties:
    BucketName: !Sub "technova-assessment-bucket-${AWS::AccountId}"
    PublicAccessBlockConfiguration:
      BlockPublicAcls: false
      BlockPublicPolicy: false
      IgnorePublicAcls: false
      RestrictPublicBuckets: false
    DeletionPolicy: Delete
```

```
AssessmentRDSSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: "Allow MySQL access from anywhere (0.0.0.0/0)"
    VpcId: !Ref AssessmentVPC
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 3306
        ToPort: 3306
        CidrIp: 0.0.0.0/0 (this shouldn't be 0.0.0.0/0)
```

2. CIS 2.2/CIS 2.3.1/ (RDS, EFS Encryption)

```
AssessmentRDSInstance:
  Type: AWS::RDS::DBInstance
  Properties:
    DBName: TechNovaDB
    AllocatedStorage: 20
    DBInstanceClass: db.t2.micro
    Engine: MySQL
    EngineVersion: "8.0"
    MasterUsername: admin
    MasterUserPassword: !Ref DBRootPassword
    PubliclyAccessible: true
    StorageEncrypted: false (Should be True)
    AutoMinorVersionUpgrade: false
    VPCSecurityGroups:
      - !GetAtt AssessmentRDSSecurityGroup.GroupId
```

AssessmentEFS:
Type: AWS::EFS::FileSystem
Properties:
Encrypted: false (this should be true)
PerformanceMode: generalPurpose

3. CIS 1.16 (IAM Wildcards)

AssessmentIAMPolicy:
Type: AWS::IAM::Policy
Properties:
PolicyName: BroadPolicy
Roles:
- !Ref AssessmentIAMRole
PolicyDocument:
Version: "2012-10-17"
Statement:
- Effect: Allow (this shouldn't be allowed)
Action: "*" (this shouldn't be set to *)
Resource: "*" (this shouldn't be set to *)

4. CIS 1.8 (Password Policy)

AssessmentIAMAccountPasswordPolicy: (password reuse must be disabled)
Type: AWS::IAM::AccountPasswordPolicy
Properties:
MinimumPasswordLength: 8 (minimum length should be 14)
RequireUppercaseCharacters: false
RequireLowercaseCharacters: false
RequireNumbers: false
RequireSymbols: false
AllowUsersToChangePassword: true
MaxPasswordAge: 90

5. CIS 3.2 (CloudTrail Validation)

AssessmentCloudTrail: (kmsID should be associated with this for this to be compliant)
Type: AWS::CloudTrail::Trail
Properties:
TrailName: TechNovaAssessmentTrail
S3BucketName: !Ref AssessmentS3Bucket
IsLogging: true
IncludeGlobalServiceEvents: true
LogFileValidationEnabled: false (log file validation must be enabled)

6. CIS 5.1.1 (EBS Encryption)

AssessmentEC2Instance: (http-token must be required)
Type: AWS::EC2::Instance
Properties:
 InstanceType: t2.micro
 ImageId: !FindInMap [RegionMap, !Ref "AWS::Region", AMI]
 SecurityGroupIds:
 - !GetAtt AssessmentEC2SecurityGroup.GroupId
 !iamInstanceProfile: !Ref AssessmentInstanceProfile
 BlockDeviceMappings:
 - DeviceName: "/dev/xvda"
 Ebs:
 VolumeSize: 8
 Encrypted: false (encryption should be enabled for this to be compliant)

7. CIS 3.6 (KMS keys should have key rotation enabled)

AssessmentKMSKey:
Type: AWS::KMS::Key
Properties:
 Description: "KMS Key with an overly permissive policy"
 EnableKeyRotation: false (should be enabled)
 KeyPolicy:
 Version: "2012-10-17"
 Statement:
 - Sid: "AllowAllActions"
 Effect: Allow
 Principal:
 AWS: "*"
 Action: "kms:*"
 Resource: "*"

8. CIS 2.1.2 - S3 buckets should have versioning enabled with MFA Delete

AssessmentS3BucketVersioning: (versioning should be enabled)
Type: AWS::S3::BucketVersioning
Properties:
 Bucket: !Ref AssessmentS3Bucket
 Status: Suspended (this should be enabled)