Security Assessment Report

HIPAA Cloud Compliance Audit

Prepared For:

Terrapin Health Systems

Prepared By:

Ty Newkirk, Cybersecurity Consultant

March 13, 2025

Confidentiality Notice:

This document contains sensitive security information. Unauthorized distribution, copying, or disclosure is strictly prohibited.

Introduction

Terrapin Health Systems is a healthcare provider that handles sensitive patient data, making compliance with the Health Insurance Portability and Accountability Act (HIPAA) a top priority. HIPAA compliance ensures the confidentiality, integrity, and availability of protected health information (PHI), reducing risks associated with unauthorized access and data breaches.This security assessment evaluates the cloudformation template used by Terrapin Health Systems against a custom HIPAA-focused CIS benchmark checklist. The assessment is based on a HIPAA-focused CIS (Center for Internet Security) checklist and reviews configurations specified in the CloudFormation template.

Control Analysis and Checklist

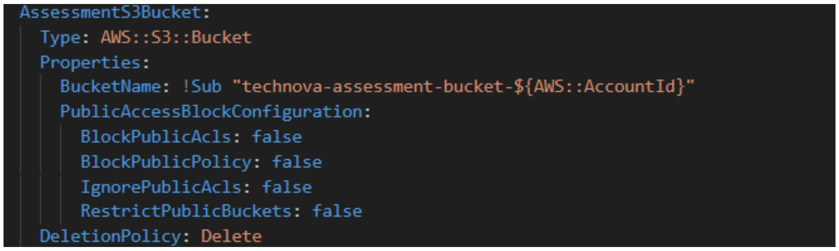
CIS Benchmark Control	Status (Compliant/Non-Compliant)
CIS 2.1.4 - S3 bucket must have Block Public Access Enabled	Non-Compliant
CIS 2.1.5 - S3 bucket must enforce secure transport (deny non-HTTPS requests)	Non-Compliant
CIS 2.2.1 - RDS instance must have encryption-at-rest enabled	Non-Compliant
CIS 2.2.3 - RDS instances must not be publicly accessible	Non-Compliant
CIS 2.3.1 - EFS file systems must be encrypted at rest	Non-Compliant
CIS 3.5 - CloudTrail logs must be encrypted at rest using KMS CMKs	Non-Compliant
CIS 3.2 - CloudTrail log file validation must be enabled	Non-Compliant
CIS 5.1.1 - EC2 instance EBS volumes must be encrypted	Non-Compliant
CIS 5.7 - The EC2 Metadata Service must enforce IMDSv2 only	Non-Compliant
CIS 1.16 - IAM policies must not grant full (“:”) administrative privileges	Non-Compliant
CIS 1.8 / 5.2 - IAM account password policy must meet HIPAA requirement (Minimum 14 Characters)	Non-Compliant
CIS 1.9 - IAM password policy must prevent password reuse	Non-Compliant
CIS 1.18 - EC2 instances must be launched with an IAM instance profile	Compliant
CIS 3.6 - Customer-managed KMS keys should have key rotation enabled	Non-Compliant
CIS 2.1.2 - S3 buckets should have versioning enabled with MFA Delete	Non-Compliant
CIS 3.1 - CloudTrail logging must be enabled	Compliant

Risk Analysis

S3 Bucket Security Risks

CIS 2.1.4 - S3 bucket must have Block Public Access Enabled (Non-Compliant)

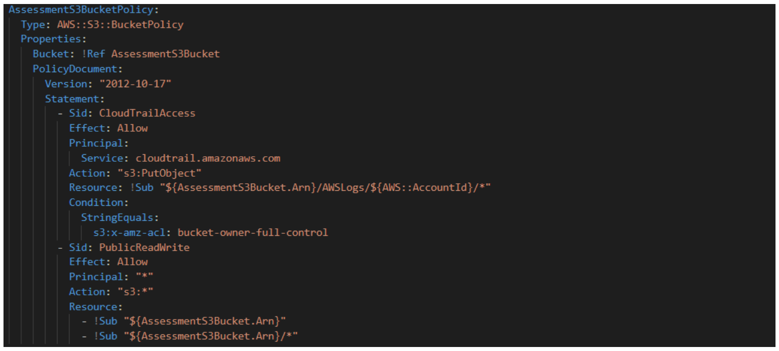
Risk: Failure to block public access increases the risk of unauthorized exposure of protected health information (PHI), violating HIPAA's Privacy Rule and Security Rule for data confidentiality.



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

CIS 2.1.5 - S3 bucket must enforce secure transport (deny non-HTTPS requests) (Non-Compliant)

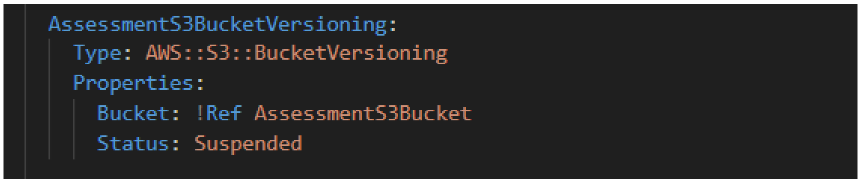
Risk: Allowing non-HTTPS traffic exposes PHI to man-in-the-middle (MITM) attacks, violating HIPAA’s requirement for data in transit encryption under the Security Rule.



```
AssessmentS3BucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref AssessmentS3Bucket
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Sid: CloudTrailAccess
          Effect: Allow
          Principal:
            Service: cloudtrail.amazonaws.com
          Action: "s3:PutObject"
          Resource: !Sub "${AssessmentS3Bucket.Arn}/AWSLogs/${AWS::AccountId}/*"
          Condition:
            StringEquals:
              s3:x-amz-acl: bucket-owner-full-control
        - Sid: PublicReadWrite
          Effect: Allow
          Principal: "*"
          Action: "s3:*"
          Resource:
            - !Sub "${AssessmentS3Bucket.Arn}"
            - !Sub "${AssessmentS3Bucket.Arn}/*"
```

CIS 2.1.2 - S3 buckets should have versioning enabled with MFA Delete (Non-Compliant)

Risk: Lack of versioning and MFA Delete increases the risk of accidental or malicious deletion of PHI, violating HIPAA’s data integrity and availability requirements.



```
AssessmentS3BucketVersioning:
  Type: AWS::S3::BucketVersioning
  Properties:
    Bucket: !Ref AssessmentS3Bucket
    Status: Suspended
```

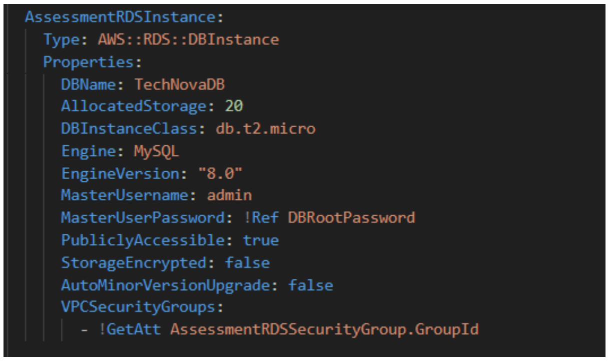
RDS Security Risks

CIS 2.2.1 - RDS instance must have encryption-at-rest enabled (Non-Compliant)

Risk: Without encryption, PHI stored in RDS databases is vulnerable to unauthorized access in the event of a data breach, violating HIPAA’s **Encryption and Data Protection Standards**.

CIS 2.2.3 - RDS instances must not be publicly accessible (Non-Compliant)

Risk: Publicly accessible RDS instances expose PHI to the internet, increasing the risk of unauthorized access, which violates HIPAA’s **Access Control and Data Protection rules**.

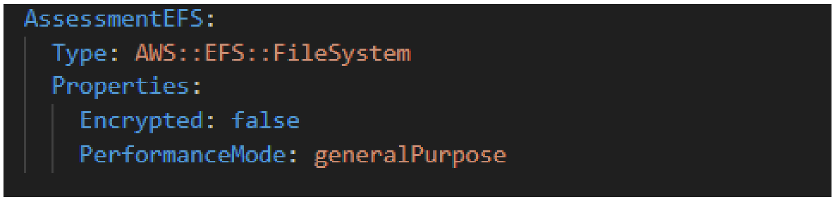


```
AssessmentRDSInstance:
  Type: AWS::RDS::DBInstance
  Properties:
    DBName: TechNovaDB
    AllocatedStorage: 20
    DBInstanceClass: db.t2.micro
    Engine: MySQL
    EngineVersion: "8.0"
    MasterUsername: admin
    MasterUserPassword: !Ref DBRootPassword
    PubliclyAccessible: true
    StorageEncrypted: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

EFS Security Risks

CIS 2.3.1 - EFS file systems must be encrypted at rest (Non-Compliant)

Risk: Unencrypted PHI stored on EFS volumes is susceptible to unauthorized access, violating HIPAA's **encryption requirements for ePHI at rest**.

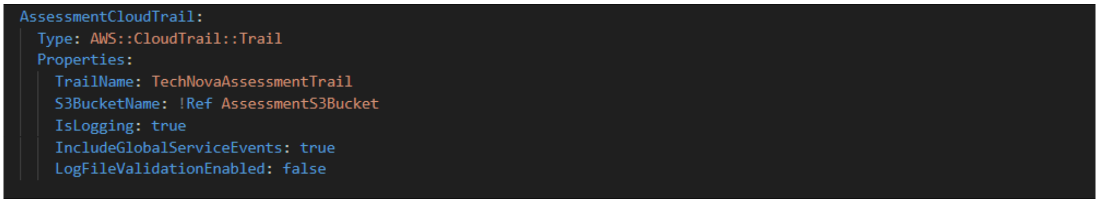


```
AssessmentEFS:
  Type: AWS::EFS::FileSystem
  Properties:
    Encrypted: false
    PerformanceMode: generalPurpose
```

CloudTrail & KMS Security Risks

CIS 3.5 - CloudTrail logs must be encrypted at rest using KMS CMKs (Non-Compliant)

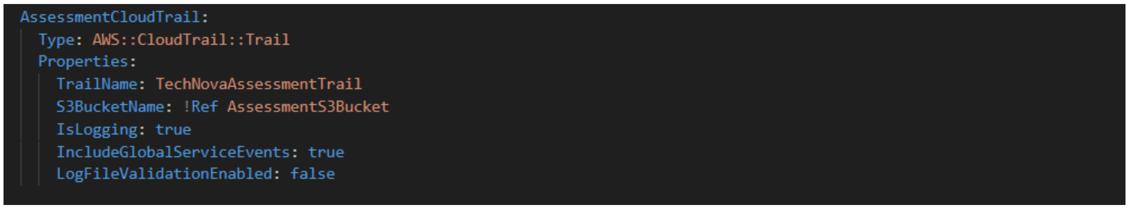
Risk: Unencrypted CloudTrail logs could lead to **log tampering**, making it harder to detect unauthorized access to PHI, violating HIPAA's **Audit Controls requirement**.



```
AssessmentCloudTrail:
  Type: AWS::CloudTrail::Trail
  Properties:
    TrailName: TechNovaAssessmentTrail
    S3BucketName: !Ref AssessmentS3Bucket
    IsLogging: true
    IncludeGlobalServiceEvents: true
    LogFileValidationEnabled: false
```

CIS 3.2 - CloudTrail log file validation must be enabled (Non-Compliant)

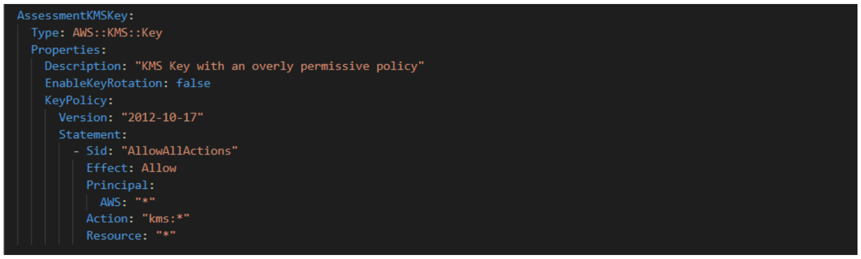
Risk: Without log validation, audit logs can be **altered or deleted**, impacting HIPAA's **auditability** and integrity requirements.



```
AssessmentCloudTrail:
  Type: AWS::CloudTrail::Trail
  Properties:
    TrailName: TechNovaAssessmentTrail
    S3BucketName: !Ref AssessmentS3Bucket
    IsLogging: true
    IncludeGlobalServiceEvents: true
    LogFileValidationEnabled: false
```

CIS 3.6 - Customer-managed KMS keys should have key rotation enabled (Non-Compliant)

Risk: Not rotating KMS keys regularly increases the risk of key compromise, potentially exposing PHI to unauthorized access, violating **HIPAA's encryption and security best practices**.



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

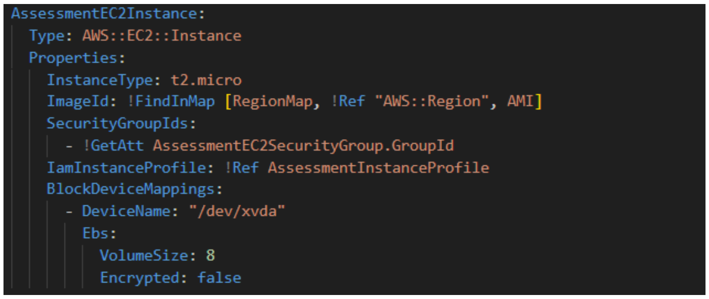
EC2 Instance Security Risks

CIS 5.1.1 - EC2 instance EBS volumes must be encrypted (Non-Compliant)

Risk: Unencrypted EBS volumes containing PHI expose patient data to unauthorized access if the disk is compromised, violating **HIPAA's encryption standards**.

CIS 5.7 - The EC2 Metadata Service must enforce IMDSv2 only (Non-Compliant)

Risk: Without **IMDSv2 enforcement**, EC2 instances are vulnerable to **metadata theft** (e.g., SSRF attacks), leading to unauthorized access to sensitive credentials and PHI, violating HIPAA's **Access Control** rules.

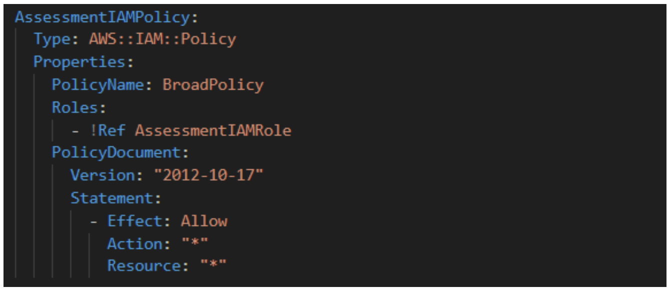


```yaml
AssessmentEC2Instance:
  Type: AWS::EC2::Instance
  Properties:
    InstanceType: t2.micro
    ImageId: !FindInMap [RegionMap, !Ref "AWS::Region", AMI]
    SecurityGroupIds:
      - !GetAtt AssessmentEC2SecurityGroup.GroupId
    IamInstanceProfile: !Ref AssessmentInstanceProfile
    BlockDeviceMappings:
      - DeviceName: "/dev/xvda"
        Ebs:
          VolumeSize: 8
          Encrypted: false
```

IAM Security Risks

CIS 1.16 - IAM policies must not grant full (“:”) administrative privileges (Non-Compliant)

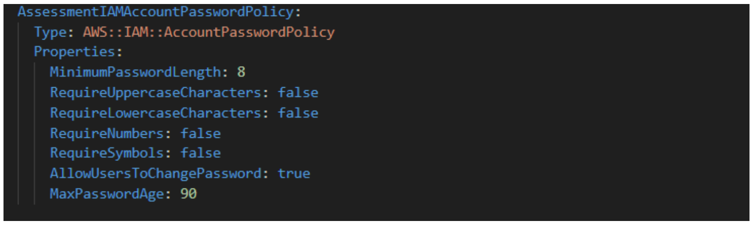
Risk: Overly permissive IAM policies increase the risk of **insider threats and privilege escalation**, violating HIPAA’s **Principle of Least Privilege (PoLP)**.



```
AssessmentIAMPolicy:
  Type: AWS::IAM::Policy
  Properties:
    PolicyName: BroadPolicy
    Roles:
      - !Ref AssessmentIAMRole
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: Allow
          Action: "*"
          Resource: "*"
```

CIS 1.8 / 5.2 - IAM account password policy must meet HIPAA requirement (Minimum 14 Characters) (Non-Compliant)

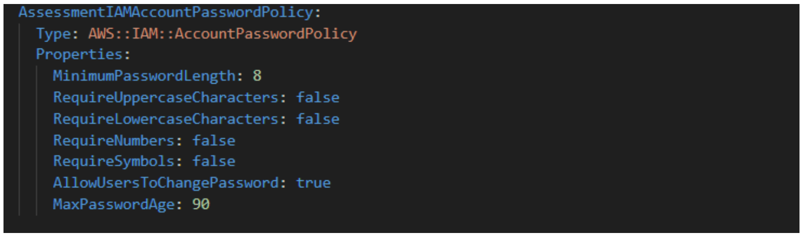
Risk: Weak password policies increase the risk of unauthorized account access, violating HIPAA’s **Access Control and Authentication requirements**.



```
AssessmentIAMAccountPasswordPolicy:
  Type: AWS::IAM::AccountPasswordPolicy
  Properties:
    MinimumPasswordLength: 8
    RequireUppercaseCharacters: false
    RequireLowercaseCharacters: false
    RequireNumbers: false
    RequireSymbols: false
    AllowUsersToChangePassword: true
    MaxPasswordAge: 90
```

CIS 1.9 - IAM password policy must prevent password reuse (Non-Compliant)

Risk: Allowing password reuse weakens security posture and increases the risk of **credential-based attacks**, violating HIPAA’s **Access Control standards**.



```
AssessmentIAMAccountPasswordPolicy:
  Type: AWS::IAM::AccountPasswordPolicy
  Properties:
    MinimumPasswordLength: 8
    RequireUppercaseCharacters: false
    RequireLowercaseCharacters: false
    RequireNumbers: false
    RequireSymbols: false
    AllowUsersToChangePassword: true
    MaxPasswordAge: 90
```

Compliant Controls

CIS 1.18 - EC2 Instances must be launched with an IAM instance

Launching EC2 instances with an IAM instance profile aligns with the CIS (Center for Internet Security) benchmarks and supports HIPAA compliance because this configuration minimizes security risks by enforcing best practices in access management, thereby meeting compliance requirements.

CIS 3.1 - CloudTrail logging must be enabled

Enabling AWS CloudTrail logging aligns with the CIS AWS Foundations Benchmark and supports HIPAA compliance by ensuring CloudTrail is enabled, organizations enhance visibility, accountability, and compliance with security best practices and HIPAA regulation

Recommendations

S3 Security Mitigations

1. **CIS 2.1.4 - Block Public Access Enabled**
   ○ **Remediation:** Enable Block Public Access settings for all S3 buckets. Review bucket policies and ACLs to ensure no public access permissions are granted.
2. **CIS 2.1.5 - Enforce Secure Transport**
   ○ **Remediation:** Configure S3 bucket policies to deny non-HTTPS requests. Implement AWS CloudFront as a proxy to enforce HTTPS for all S3 traffic.
3. **CIS 2.1.2 - Versioning with MFA Delete**
   ○ **Remediation:** Enable versioning on all S3 buckets and configure MFA Delete to require multi-factor authentication for version deletion actions.

RDS Mitigations

4. **CIS 2.2.1 - Encryption-at-Rest Enabled**
   ○ **Remediation:** Enable encryption at rest for all RDS instances using AWS KMS. For existing databases, consider taking snapshots, modifying them to enable encryption, and restoring from the snapshot.

5. **CIS 2.2.3 - RDS Instances Not Publicly Accessible**
    - **Remediation:** Ensure RDS instances are not publicly accessible. Update the RDS instance's public accessibility setting and configure security groups to restrict access to trusted IPs or VPC.

EFS Mitigations

6. **CIS 2.3.1 - EFS File Systems Encrypted at Rest**
    - **Remediation:** Enable encryption for all EFS file systems. Use AWS-managed keys or customer-managed KMS keys for encryption.

CloudTrail & KMS Security Mitigations

7. **CIS 3.5 - CloudTrail Logs Encrypted at Rest**
    - **Remediation:** Configure CloudTrail to use KMS customer-managed keys (CMKs) for log encryption. Verify existing logs are encrypted.
8. **CIS 3.2 - Log File Validation Enabled**
    - **Remediation:** Enable log file validation for CloudTrail to ensure integrity and prevent tampering.
9. **CIS 3.6 - KMS Key Rotation Enabled**
    - **Remediation:** Enable automatic key rotation for customer-managed KMS keys to ensure keys are rotated annually or more frequently.

EC2 Security Mitigations

10. **CIS 5.1.1 - EBS Volumes Encrypted**
    - **Remediation:** Enable encryption for all EBS volumes attached to EC2 instances. For existing unencrypted volumes, create snapshots, enable encryption, and create new encrypted volumes from the snapshots.
11. **CIS 5.7 - IMDSv2 Enforcement**
    - **Remediation:** Configure EC2 instances to use IMDSv2 by updating instance metadata service settings. Review applications for compatibility with IMDSv2.

IAM Mitigations

12. **CIS 1.16 - IAM Policies Not Granting Full Admin Privileges**
    - **Remediation:** Review and restrict IAM policies to ensure no full administrative privileges are granted. Implement least privilege principles by creating custom roles with only necessary permissions.
13. **CIS 1.8 / 5.2 - Password Policy Meets HIPAA Requirements**
    - **Remediation:** Update IAM account password policy to require a minimum of 14 characters. Enforce complexity requirements (e.g., a mix of uppercase, lowercase, numbers, and special characters).
14. **CIS 1.9 - Prevent Password Reuse**
    - **Remediation:** Update IAM password policy to prevent password reuse by enforcing a password history that remembers the last 5 passwords.

Compliance Posture Summary of Terrapin Health Systems

Terrapin Health Systems currently has multiple non-compliant security controls across its AWS infrastructure, posing significant risks to the confidentiality, integrity, and availability of Protected Health Information (PHI). Key compliance gaps include misconfigured S3 buckets, unencrypted RDS and EFS storage, insufficient IAM security policies, and lack of key security features such as CloudTrail log validation and KMS key rotation. These deficiencies violate critical HIPAA Security Rule requirements, including access control, encryption, auditability, and least privilege enforcement.

To improve its security posture and achieve compliance, Terrapin Health Systems must take immediate action to remediate these vulnerabilities. Recommended measures include enabling S3 Block Public Access, enforcing secure transport, encrypting all storage solutions, implementing strong IAM policies, and ensuring CloudTrail log integrity. Addressing these gaps will enhance data protection, mitigate security risks, and align the organization with HIPAA's regulatory requirements.While remediation efforts are underway, the organization's current security posture remains **non-compliant** with HIPAA standards, exposing it to potential regulatory penalties and data breach risks. Swift implementation of the proposed security controls is essential to achieving compliance and safeguarding patient data.