Protecting Patient Data under HIPAA/HITECH: Policy Recommendations for the Center

DSCI-519

Semester Project

By:

Prashant Gupta

USC ID: 3904-7127-87

PGUPTA06@USC.EDU

Department of Data Science

Viterbi School of Engineering

University of Southern California

Los Angeles, California

Executive Summary

This report conducts an evaluation of The Center's responsibilities in safeguarding Protected Health Information (PHI) within the regulatory frameworks established by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. As a bioinformatics company specializing in molecular pathology and clinical research, The Center operates within a multifaceted ecosystem encompassing third-party platforms such as Cartagenia and cloud services offered by Amazon Web Services.

The assessment initiates with a detailed examination of the privacy and security policies pertinent to The Center, including the HIPAA Security Rule, the Cartagenia Data Security Policy, and the compliance standards of AWS. Essential requirements include data encryption, role-based access control, and physical and technical safeguards for PHI. A comprehensive threat analysis reveals significant risks, including unauthorized access, social engineering, insider threats, and inadequate encryption practices.

Access control policies are articulated within enforceable frameworks, employing Role-Based Access Control (RBAC), Discretionary Access Control (DAC), and Mandatory Access Control (MAC). These policies delineate user roles, resource classifications, and access permissions to ensure the confidentiality, integrity, and proper availability of sensitive data. Furthermore, this report identifies and addresses areas where current policies are deficient, particularly in auditing, availability, and the mitigation of insider threats.

To address these deficiencies, the report recommends implementing several enhancements, including advanced encryption protocols, multi-factor authentication, security awareness training, and comprehensive logging and monitoring systems. Successfully adopting these measures will enhance The Center's compliance with HIPAA regulations, mitigate threats to PHI, and establish a more robust security posture.

In conclusion, this report underscores the necessity of aligning technical, administrative, and physical controls with regulatory mandates and evolving threats to protect sensitive health information effectively.

CONTENTS

Chapter	Page no.
Title page	i
Executive Summary	ii
1. Introduction	1
1.1. Purpose	2
1.2. Scope	2
1.3. Importance of Privacy and Security Policies	2
2. Privacy and Information Security Policies	3
2.1. HIPAA and NIST Guidelines	4
2.2. The Center's Existing Policies	5
2.2.1. Access Control and User Management	5
2.2.2. Data Security Measures	5
2.2.3. Data Retention and Storage	5
2.2.4. Data Retention and Storage	5
2.3. Cartagenia and AWS Considerations	6
2.3.1. Cartagenia's data security policy	6
2.3.2. AWS HIPAA compliance guidelines	6
3. Threat Analysis	7
3.1. Unauthorized Access	8
3.2. Data Breaches	8
3.3. Insider Threats	8
3.4. Malware and Ransomware Attacks	8
3.5. Social Engineering	9
4. Access Control Policy Development	10
4.1. User and Resource Identification	11
4.2. Access Control Models	11
4.2.1. RBAC	11
4.2.2. MAC	11
4.2.3. DAC	12
4.3. User-Role Assignments	13
4.4. Role-Permission Mappings	13

5. Additional Requirements	**14**
5.1. Data Availability Measures	**15**
5.1.1. Backup and Recovery	**15**
5.1.2. Redundancy	**15**
5.1.3. Disaster Recovery	**15**
5.2. Audit and Accountability Procedures	**15**
5.2.1. Access Logging	**15**
5.2.2. Change Management	**15**
5.2.3. Regular Audits	**16**
5.2.4. Incident Response	**16**
5.3. Encryption Standards for Data in Transit and at Rest	**16**
5.3.1. Data in Transit	**16**
5.3.2. Data at Rest	**16**
5.3.3. Key Management	**16**
5.3.4. Encryption Algorithm	**16**
6. Threat Space Analysis	**17**
7. Additional Control	**19**
7.1. Administrative Safeguards	**20**
7.1.1. Security Awareness Training	**20**
7.1.2. Incident Response Plan	**20**
7.1.3. Vendor Management	**20**
7.2. Physical Safeguards	**20**
7.2.1. Biometric Access Controls	**20**
7.2.2. Environmental Controls	**20**
7.2.3. Asset Management	**20**
7.3. Technical Safeguards	**20**
7.3.1. Intrusion Detection and Prevention Systems	**20**
7.3.2. Multi-Factor Authentication	**20**
7.3.3. Data Loss Prevention	**20**
7.3.4. Encryption	**21**
7.3.5. Secure Configuration Management	**21**
7.3.6. Advanced Threat Protection	**21**
Conclusion & References	**23**

Chapter One

Introduction

1.1 Purpose:

The objective of this report is to assess The Center's compliance obligations under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act about the safeguarding of Protected Health Information (PHI). This assessment encompasses a thorough analysis of existing policies, the identification of compliance deficiencies, and the examination of vulnerabilities associated with protecting sensitive health data. Furthermore, the report provides specific, actionable recommendations to enhance data security and ensure confidentiality, integrity, and availability of health information.

1.2 Scope:

This report analyzes The Center, a bioinformatics organization that employs Cartagenia's clinical informatics platform alongside Amazon Web Services (AWS) for cloud storage and data analysis. The focus of this analysis includes a comprehensive review of documents pertinent to the Health Insurance Portability and Accountability Act (HIPAA), specifically the Security Rule, the Cartagenia Data Security Policy, and AWS compliance guidelines. The report identifies potential threats to protected health information (PHI) and converts comprehensible policies into access control mechanisms, notably Role-Based Access Control (RBAC). Furthermore, it recommends additional administrative, physical, and technical measures to ensure a robust security framework.

1.3 Importance of Privacy and Security Policies:

Privacy and security policies are essential for protecting protected health information (PHI) from unauthorized access and breaches as entities subject to the Health Insurance Portability and Accountability Act (HIPAA), The Center and its collaborators must meet strict regulatory standards. Noncompliance can lead to significant financial penalties and damage to reputation.

Effective policies are crucial for safeguarding patient privacy and maintaining trust in healthcare institutions. With the rise of cyber threats and cloud computing, adopting strong security measures that align with HIPAA regulations is a legal requirement and a top priority for the organization.

Chapter Two

Privacy and Information Security Policies

2.1 HIPAA and NIST Guidelines:

The HIPAA Security Rule defines Protected Health Information (PHI) as individually identifiable health information created, collected, transmitted, or maintained by a HIPAA-covered entity about the provision of healthcare, payment for healthcare services, or use in healthcare operations.

Key points include:

- PHI includes 18 specific identifiers; if these identifiers are removed, the information is considered de-identified protected health information, which is not subject to HIPAA Rules.
    1. Names (Full or last name and initial)
    2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
    3. Dates (other than year) directly related to an individual
    4. Phone Numbers
    5. Fax numbers
    6. Email addresses
    7. Social Security numbers
    8. Medical record numbers
    9. Health insurance beneficiary numbers
    10. Account numbers
    11. Certificate/license numbers
    12. Vehicle identifiers (including serial numbers and license plate numbers)
    13. Device identifiers and serial numbers;
    14. Web Uniform Resource Locators (URLs)
    15. Internet Protocol (IP) address numbers
    16. Biometric identifiers, including finger, retinal and voice prints
    17. Full face photographic images and any comparable images

18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

- The HIPAA Security Rule mandates that covered entities implement appropriate administrative, physical, and technical safeguards to protect electronic PHI.
- NIST Special Publication 800-66 guides on implementing the HIPAA Security Rule, including risk assessment, access control, audit controls, and integrity controls.

2.2 The Center's Existing Policies:

2.2.1 Access Control and User Management:

- Access to computing equipment granted by Bioinformatics Director or Supervisor.
- User groups defined with specific access rights (root, bioinfo, bioinfoclin, clinical, research, hla, smbgroup).
- Reserved usernames established for various roles and functions.

2.2.2 Data Security Measures:

- Clinical data transfers occur within Hospital's network, with exceptions for specific cloud services.
- Physical access to server rooms restricted and logged.
- HIPAA-compliant hardware used, with segregation of clinical and research data.

2.2.3 Data Transfer and Encryption:

- Data transferred outside Hospital network encrypted using SFTP, HTTPS, and rsync via SSH.
- Connections to AWS and Cartagenia BENCH Lab NGS made via HTTPS.
- Remote access to servers uses SSH for secure data communication.

2.2.4 Data Retention and Storage:

- Raw data stored indefinitely in AWS Glacier.
- Data retention periods defined as temporary, short-term (30 days), intermediate (1 year), long-term (7 years or until patient reaches 21), and indefinite.
- Checksums calculated and confirmed for data transfers between sites.

2.3 Cartagenia and AWS Considerations

2.3.1 Cartagenia's data security policy:

- Customers retain ownership and control of PHI entered into the Bench platform.
- Data transfers use industry-standard encryption (SSL/TLS).
- Access to customer data is strictly limited and logged.

2.3.2 AWS HIPAA compliance guidelines:

- HIPAA-eligible services offered for storing, processing, and transmitting PHI.
- Customers responsible for implementing appropriate security controls.
- Features provided include encryption, access controls, and auditing to help meet HIPAA requirements.
- AWS Business Associate Addendum (BAA) available for HIPAA-covered entities and business associates.
- HIPAA-eligible services include Amazon EC2, S3, RDS, DynamoDB, and others.

Chapter Three

Threat Analysis

The protection of Protected Health Information (PHI) is crucial for healthcare organizations. Here's a comprehensive summary of potential threats to PHI:

3.1 Unauthorized Access

Unauthorized access to PHI poses a significant risk to patient privacy and data security. This threat can manifest in several ways:

- Weak access controls allowing unauthorized users to view or modify PHI
- Insufficient authentication mechanisms leading to compromised user accounts
- Improper session management, enabling unauthorized access to active sessions
- Misconfigured permissions granting excessive access rights to users

The Center must enforce strict access controls, use multi-factor authentication, and conduct regular access audits to reduce this threat.

3.2 Data Breaches

Data breaches can result in large-scale exposure of PHI. Potential scenarios include:

- Interception of unencrypted data during transmission
- Theft or loss of physical devices containing PHI
- Exploitation of vulnerabilities in the network or application infrastructure
- Accidental exposure of PHI through misconfigurations or human error

To combat this threat, the Center must encrypt data both at rest and in transit, implement secure backup procedures, and regularly assess and patch vulnerabilities.

3.3 Insider Threats

Insider threats are particularly challenging as they involve individuals with legitimate access to PHI. These threats can include:

- Malicious employees intentionally accessing PHI
- Negligent staff members accidentally exposing or mishandling PHI
- Compromised user accounts used by external attackers to access PHI

Addressing insider threats requires a mix of technical controls, employee training, and strong monitoring and auditing processes.

3.4 Malware and Ransomware Attacks

Malware and ransomware pose significant risks to the integrity and availability of PHI:

- Ransomware encrypting PHI and demanding payment for decryption
- Malware designed to exfiltrate PHI from compromised systems

- Advanced persistent threats (APTs) establishing a long-term presence in the network

The Center should implement comprehensive malware protection, conduct regular system updates, and establish strong backup and recovery procedures to mitigate these threats.

3.5 Social Engineering

Social engineering attacks exploit human psychology to gain unauthorized access to PHI:

- Phishing emails tricking employees into revealing login credentials.
- Pretexting attacks where attackers impersonate authorized personnel.
- Baiting attacks using physical media to spread malware.

Organizations must provide ongoing security awareness training for all employees to address social engineering threats. They should establish an email filtering system and create clear procedures for verifying identities and requests.

.

The Center can create a comprehensive security strategy to safeguard PHI and ensure HIPAA compliance by identifying and addressing potential threats. Regular risk assessments, employee training, and ongoing monitoring are crucial for an effective PHI protection program.

Chapter Four

Access Control Policy Development

4.1 User and Resource Identification

The Center's structure includes several key user roles and protected resources that need to be secured. While we are currently focusing on the main categories, there are possibilities for further divisions.

Users/Roles:

- IT Director
- Bioinformatics Director
- Bioinformatics Supervisor
- System Administrator
- Lab Manager
- Medical Director
- Other Employees

Protected Resources:

- Clinical data
- Non-clinical data
- Research data

4.2 Access Control Models

The Center can use Role-Based Access Control (RBAC), Mandatory Access Control (MAC), and Discretionary Access Control (DAC) to ensure comprehensive protection of PHI.

4.2.1 Role-Based Access Control (RBAC)

RBAC structure for the Center:

- Root
- Bioinfo
- Bioinfoclin
- Clinical
- Research
- Hla
- Smbgroup

4.2.2 Mandatory Access Control (MAC)

MAC can be implemented with the following security levels, from highest to lowest priority:

Security Level	Description	Access Control
Directors	The highest level of access includes the IT Director and Bioinformatics Director.	Full access to all data and resources.
Administrators	Access for System Administrators and designated personnel.	Manage user access and system configurations.
Users	General users with specific access rights based on their roles.	Limited access to relevant data only.
Researchers	Users conducting research without access to clinical data or pipelines.	Access to research data only; no clinical data access.

Dominance relationship: *Directors* ***dom*** *Administrators* ***dom*** *Users* ***dom*** *Researchers*

4.2.3 Discretionary Access Control (DAC)

- Non- clinical

Object / Subject	Non Clinical data
Root	Read, Write
Bioinfo	Read, Write
Sbmgroup	Read

- Clinical data

Object / Subject	Clinical data
Root	Read, Write
Bioinfo	Read
Sbmgroup	Read, Write
Bioinfoclin	Read
Clinical	Read
Hla	Read, Write

- Research data

Object / Subject	Research data
Root	Read, Write
Research	Read, Write
Hla	Read, Write

4.3 User-Role Assignments

User/Role	Assigned Role
IT Director	Root
Bioinformatics Director	Root, Research
Bioinformatics Supervisor	Root, Research
System Administrator	Root
Lab Manager	Bioinfoclin
Medical Director	Clinical
Other Employees	Bioinfo, Smbgroup

4.4 Role-Permission Mappings

Role	Permissions
Root	Read/Write access to Non-clinical software/data, Clinical data, and Research data.
Bioinfo	Read/Write access to Non-clinical software/data.
Bioinfoclin	Read/Write access to Clinical data.
Clinical	Read/Write access to Clinical data.
Research	Read/Write access to Research data.
Hla	Read/Write access to Clinical and Research data.
Smbgroup	Read access to Non-clinical software/data.

By enforcing these access control policies, the Center can ensure that protected health information (PHI) is safeguarded and only accessible to personnel authorized according to their roles and responsibilities.

Chapter Five

Additional Requirements

Access control policies are critical for data protection; however, several additional requirements must be addressed to ensure a comprehensive approach to security for Protected Health Information (PHI) at the Center. These requirements complement the access control policies and are essential for maintaining compliance with the Health Insurance Portability and Accountability Act (HIPAA).

5.1 Data Availability Measures

5.1.1 Backup and Recovery:

- Implement a robust backup system using AWS Glacier for long-term storage of raw NGS data.
- Establish a clear data retention policy, with different periods for temporary, short-term, intermediate, and long-term storage.
- Ensure that software and annotations required for data analysis are retained and versioned.

5.1.2 Redundancy:

- Utilize RAID configurations for storage redundancy, as specified by the Bioinformatics Director.
- Implement geographically distributed backups to protect against localized disasters.

5.1.3 Disaster Recovery:

- Develop and regularly test a comprehensive disaster recovery plan.
- Ensure that data can be restored from AWS Glacier in case of local data loss.

5.2 Audit and Accountability Procedures

5.2.1 Access Logging:

- Implement detailed logging of all access to PHI, including user identity, time of access, and actions performed.
- Regularly review access logs to detect any unauthorized or suspicious activities.

5.2.2 Change Management:

- Establish a formal change management process for all systems handling PHI.

- Document and track all changes to software, hardware, and configurations.

5.2.3 Regular Audits:

- Conduct periodic internal audits of security measures and access controls.
- Perform annual HIPAA compliance audits.

5.2.4 Incident Response:

- Develop and maintain an incident response plan for potential data breaches or security incidents.
- Conduct regular training and drills for the incident response team.

5.3 Encryption Standards for Data in Transit and at Rest

5.3.1 Data in Transit:

- Use HTTPS for all web-based connections, including AWS and Cartagenia BENCHLab NGS.
- Employ SFTP or rsync via SSH for file transfers outside the Hospital network.
- Ensure all remote access to servers occurs via SSH.

5.3.2 Data at Rest:

- Implement strong encryption for all PHI stored on local servers and in cloud storage.
- Use AWS Key Management Service (KMS) to manage encryption keys in the cloud environment.

5.3.3 Key Management:

- Establish a robust key management system to securely generate, store, and rotate encryption keys.
- Implement strict access controls for encryption keys, limiting access to authorized personnel only.

5.3.4 Encryption Algorithms:

- Use industry-standard encryption algorithms, e.g., AES-256 for both data in transit and at rest.
- Regularly review and update encryption standards to align with current best practices and NIST recommendations.

Chapter Six

Threat Space Analysis

6.1 Threat Space Analysis:

- Unauthorized access is largely mitigated through RBAC and MAC implementations.
- Data breaches are partially addressed by DAC policies and data encryption in transit.
- Insider threats are partially mitigated by role-based permissions limiting access scope.
- Physical device theft/loss risks require additional mitigation measures.
- Comprehensive monitoring and auditing mechanisms are lacking for insider threats.
- Social engineering attacks are not directly addressed, leaving human vulnerabilities exposed.
- The policies do not specifically address malware and ransomware attacks.
- Physical security measures are not fully integrated into the access control framework.
- Data availability concerns are insufficiently addressed, with a focus mainly on confidentiality and integrity.
- No specific measures to detect and mitigate advanced persistent threats.
- Risks associated with third-party integrations (Cartagenia and AWS) are not fully addressed.
- Additional controls and policies are needed to address remaining vulnerabilities and partially addressed threats.

Chapter Seven

Additional Controls

7.1 Administrative Safeguards

7.1.1 Security Awareness Training:

- Implement a comprehensive security awareness program for all employees.
- Conduct regular phishing simulations to test and improve staff vigilance.
- Provide role-specific training for employees handling sensitive data.

7.1.2 Incident Response Plan:

- Develop and regularly test an incident response plan for data breaches.
- Establish clear roles and responsibilities for the incident response team.

7.1.3 Vendor Management:

- Implement a robust vendor risk assessment process.
- Regularly review and update Business Associate Agreements with Cartagenia and AWS.

7.2 Physical Safeguards

7.2.1 Biometric Access Controls:

- Install biometric authentication systems for server rooms and sensitive areas.
- Implement multi-factor authentication for physical access to critical infrastructure.

7.2.2 Environmental Controls:

- Ensure proper temperature and humidity controls in server rooms.
- Install fire suppression systems and water detection sensors.

7.2.3 Asset Management:

- Maintain an up-to-date inventory of all devices containing or accessing PHI.
- Implement secure disposal procedures for decommissioned hardware.

7.3 Technical Safeguards

7.3.1 Intrusion Detection and Prevention Systems (IDS/IPS):

- Deploy network-based IDS/IPS to monitor for suspicious activities.
- Implement host-based IDS on critical servers to detect unauthorized changes.

7.3.2 Multi-Factor Authentication (MFA):

- Enforce MFA for all user accounts, especially those with elevated privileges.
- Implement risk-based authentication for accessing sensitive data.

7.3.3 Data Loss Prevention (DLP):

- Deploy DLP solutions to monitor and prevent unauthorized data exfiltration.
- Implement content-aware DLP policies to identify and protect PHI.

7.3.4 Encryption:

- Utilize AWS Key Management Service (KMS) to manage encryption keys.
- Implement end-to-end encryption for data in transit and at rest.
- Use field-level encryption for sensitive database columns.

7.3.5 Secure Configuration Management:

- Implement automated configuration management tools to ensure consistent security settings.
- Regularly scan for and remediate misconfigurations and vulnerabilities.

7.3.6 Advanced Threat Protection:

- Deploy next-generation firewalls with application-level filtering capabilities.
- Implement sandboxing technologies for analyzing suspicious files and URLs.

By implementing these additional controls, the Center can significantly enhance its security posture, address any remaining vulnerabilities, and ensure comprehensive protection of Protected Health Information (PHI) in accordance with HIPAA regulations.

CONCLUSION
&
REFERENCES

Conclusion:

The Center is responsible for protecting patient data under HIPAA/HITECH regulations, which requires a comprehensive security approach. Key areas for improvement include implementing robust access control policies, such as Role-Based Access Control (RBAC), Mandatory Access Control (MAC), and Discretionary Access Control (DAC). These measures ensure that only authorized personnel can access sensitive information.

In addition to access control, The Center must prioritize data availability, secure communication with third-party services like Cartagenia and AWS, network segmentation, and thorough audit procedures. Implementing multi-factor authentication, enhancing physical security, and providing ongoing security training for staff are crucial for mitigating potential threats.

The threat landscape is diverse, encompassing risks from data breaches to insider threats. Adopting a defense-in-depth strategy will significantly strengthen The Center's security posture. Ultimately, protecting patient data is essential for maintaining patient trust and ensuring the integrity of health information. By implementing these measures and fostering a culture of security awareness, The Center can excel in secure bioinformatics practices.

References:

[1] HIPAA Security Rule and related NIST guidelines (NIST Special Publication 800-66)

[2] Cartagenia Data Security Policy

[3] AWS HIPAA compliance guidelines

[4] Amazon Web Services – Using AWS for Disaster Recovery

[5] Amazon Web Services – Architecting for HIPAA Security and Compliance on Amazon Web Services

[6] National Institute of Standards and Technology - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

[7] HIPAA Journal - What is considered protected health information under HIPAA (https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/)