Project Title: "Cybersecurity Policy and HIPAA Compliance for The Center"

Author's Name: Kamalesh Jayapandiaraj Arumugam

Course Name and Code: DSCI 519 – Foundations and Policy for Information Security

Viterbi School of Engineering
University of Southern California
Los Angeles, CA
karumuga@usc.edu

Submission Date: December 04, 2024

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

Index

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

VI. Additional Security Requirements
- a. Availability measures
- b. Data integrity controls
- c. Audit and monitoring capabilities

VII. Gap Analysis
- a. Threat areas not fully addressed by access control policies
- b. Assessment of residual risks

VIII. Recommended Additional Controls
- a. Administrative controls
- b. Physical controls
- c. Technical controls

IX. Implementation Roadmap
- a. Prioritized list of recommended actions
- b. Estimated timelines and resource requirements

X. Conclusion

XI. References

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

I. Executive Summary

The Hospital Center (HC), a bioinformatics company specializing in molecular pathology, clinical genetic labs, and research, must prioritize HIPAA compliance to protect sensitive patient health information. This report analyzes HC's current data security policies and recommends improvements to ensure full HIPAA compliance and robust protection of electronic protected health information (ePHI).

Key findings:

1. HC has implemented several important security measures, including:
    - Strict access controls with defined user groups and roles
    - Data encryption during transfers and remote access
    - De-identification procedures for shared data
    - Comprehensive data retention and backup policies
2. However, some gaps in the current policies require attention:
    - Lack of a formal risk assessment process
    - Incomplete incident response and disaster recovery procedures
    - Insufficient detail on workforce security training
3. Primary recommendations:
    - Implement a formal, ongoing risk assessment program
    - Enhance access control policies by adopting role-based access control (RBAC) and mandatory access control (MAC) models
    - Develop comprehensive incident response and disaster recovery plans
    - Expand security awareness and training programs for all staff
    - Strengthen policies for business associate agreements and third-party vendor management
    - Implement regular security audits and evaluations

By addressing these recommendations, HC can significantly improve its HIPAA compliance posture and better protect patient data from evolving cybersecurity threats. This will not only ensure regulatory compliance but also enhance patient trust and the organization's reputation in handling sensitive genetic and health information.

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

II. Introduction

The Center and Its Data Management

The Hospital Center (HC), also known as "the Center," is a bioinformatics company specializing in molecular pathology, clinical genetic labs, and research. The Center heavily relies on next-generation sequencing (NGS) data for its operations and patient care. To manage this vast amount of sensitive genetic information, the Center utilizes two key external services:

1. Amazon Web Services (AWS): The Center's data is managed and stored in the cloud using AWS, which provides HIPAA-compliant storage and processing capabilities

2. Cartagenia: The Center has contracted with Cartagenia to provide a clinical informatics platform used for data analysis. This arrangement involves a complex data ownership and security structure, as Cartagenia has an agreement with AWS, and the Center has an agreement with Cartagenia

HIPAA Context

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes federal standards for protecting sensitive health information. The HIPAA Security Rule specifically focuses on safeguarding electronic protected health information (ePHI)

As a healthcare provider that transmits health information electronically, the Center is considered a covered entity under HIPAA and must comply with its regulations

Key requirements of the HIPAA Security Rule include:

- Ensuring the confidentiality, integrity, and availability of all ePHI
- Protecting against reasonably anticipated threats or hazards to ePHI security
- Safeguarding against impermissible uses or disclosures of ePHI
- Ensuring compliance by the workforce

The objective of this report is to:

1. Review the Center's existing information protection policies and compare them with NIST guidelines and HIPAA requirements.
2. Identify potential threats to the protected information and assess whether current policies adequately address the entire threat space.
3. Develop enforceable security policies by applying appropriate cybersecurity frameworks studied in class.
4. Recommend additional controls and security improvements where the current policies and practices may be deficient.

By conducting this comprehensive analysis, we aim to enhance the Center's HIPAA compliance posture and strengthen its overall data security practices to better protect sensitive patient information.

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

III. Review of Information Protection Policies

A. NIST Guidelines (NIST 800-66)

a. Security management process

The HIPAA Security Rule requires covered entities to implement policies and procedures to prevent, detect, contain, and correct security violations. NIST recommends conducting risk assessments, implementing a risk management program, and maintaining formal security policies

b. Assigned security responsibility

Organizations must identify a security official responsible for developing and implementing security policies and procedures. This individual should have the authority to make decisions regarding information security.

c. Workforce security

NIST guidelines emphasize implementing procedures for authorizing workforce access to EPHI, as well as establishing termination procedures and sanctions for policy violations. Background checks and confidentiality agreements may also be appropriate.

d. Information access management

Access to EPHI should be restricted based on job responsibilities. NIST recommends implementing role-based access controls and regularly reviewing user access rights.

e. Security awareness and training

All workforce members should receive appropriate training on security policies and procedures. NIST suggests providing both initial and ongoing security awareness education.

f. Security incident procedures

Organizations must implement policies and procedures to address security incidents. This includes identifying, responding to, mitigating harm from, and documenting security incidents.

g. Contingency planning

NIST recommends developing and implementing a data backup plan, disaster recovery plan, and emergency mode operation plan. Regular testing of these plans is also advised.

h. Evaluation

Covered entities should perform periodic technical and non-technical evaluations to ensure security policies and procedures meet the requirements of the Security Rule. NIST suggests both internal and external security audits.

i. Business associate agreements

When a covered entity engages a business associate to create, receive, maintain, or transmit EPHI, a written contract or agreement is required that establishes the permitted uses and disclosures of such information.

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

B. Hospital Center (HC) Policies

a. Data security and confidentiality

- The Bioinfo rmatics Director is responsible for data security and confidentiality decisions at HC in accordance with hospital policies
- All personnel must follow Hospital and Hospital IT policies regarding data access, confidentiality and security
- Users with access to clinical data must undergo HIPAA training

b. Access rights and user groups

- Access to computing equipment is granted by the Bioinformatics Director or Supervisor
- User groups include: root, bioinfo, bioinfoclin, clinical, research, hla, and smbgroup
- Each group has specific access rights and permissions defined (e.g. bioinfoclin can access clinical data and modify clinical software)

c. Physical security measures

- Access to the IDF/HC Server Room is restricted to authorized personnel and logged
- The server room has locked keyed entry
- At USC HPCC, there are at least three biometric security measures for physical access

d. Data transfer and transmission policies

- Clinical data is transferred within the Hospital's network, except for certain cloud services
- Data transferred outside the network is encrypted (e.g. SFTP, HTTPS, SSH)
- AWS and Cartagenia are used for cloud storage/processing with HIPAA-compliant services

e. Data retention and archiving

- Raw NGS data is stored indefinitely in AWS Glacier as the primary archive
- Processed files are kept locally for at least 1-year post-processing
- Software and annotations required to regenerate analyses are retained long-term

f. Incident response and disaster recovery

- The document does not provide specific details on incident response or disaster recovery procedures for HC
- It mentions that the Bioinformatics Director or designee may perform data recovery from archives in certain circumstances

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

C. Comparative Analysis

a. Areas of alignment between NIST and HC policies

1. Security Management Process: Both NIST and HC emphasize the importance of a comprehensive security management process. HC has designated the Bioinformatics Director as responsible for data security decisions, aligning with NIST's recommendation for assigned security responsibility
2. Access Control: NIST recommends implementing role-based access controls, which HC has implemented through defined user groups and roles (e.g., root, bioinfo, clinical, research)
3. Encryption: Both NIST and HC policies stress the importance of encryption for data transfers outside the network. HC uses encrypted protocols like SFTP, HTTPS, and SSH
4. Physical Security: NIST guidelines and HC policies both address physical security measures. HC restricts and logs access to server rooms, aligning with NIST recommendations
5. Training: Both emphasize the importance of security awareness training. HC requires HIPAA compliance training for all users with access to clinical data

b. Gaps or discrepancies identified

1. Risk Assessment: NIST strongly recommends conducting regular risk assessments, but the HC policies document does not explicitly mention a formal, ongoing risk assessment process
2. Incident Response: While NIST provides detailed guidelines on security incident procedures, the HC document lacks specific information on incident response and disaster recovery procedures
3. Contingency Planning: NIST emphasizes the need for comprehensive contingency planning, including data backup, disaster recovery, and emergency mode operation plans. HC's policies focus mainly on data retention and backup, but lack detail on disaster recovery and emergency operations
4. Evaluation: NIST recommends periodic technical and non-technical evaluations of security policies and procedures. HC's document does not mention a formal evaluation process
5. Business Associate Agreements: NIST emphasizes the importance of business associate agreements, but HC's policies do not provide detailed information on managing these relationships beyond mentioning agreements with AWS and Cartagenia
6. Workforce Security: While HC has policies on access rights, NIST provides more comprehensive guidance on workforce security, including procedures for authorization, termination, and sanctions for policy violations

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

IV. Threat Assessment

a. Potential internal threats

Healthcare organizations face significant risks from within, often due to human error or malicious intent. Key internal threats include:

1. Careless Employees: Unintentional data security compromises, such as mishandling passwords or leaving systems unattended.
2. Malicious Insiders: Employees motivated by financial gain, grievances, or ideological reasons who may deliberately access or misuse sensitive data.
3. Unauthorized Access: Staff accessing patient records outside their job scope, violating privacy policies.
4. Unencrypted Communication Channels: Use of insecure methods like email or SMS for transmitting sensitive information.
5. Phishing and Social Engineering Attacks: Employees tricked into divulging credentials or installing malicious software.
6. Improper Document Handling: Physical PHI (Protected Health Information) disposed of improperly, leading to potential data breaches.

b. External threats

External threats exploit vulnerabilities in systems, networks, and human behaviors. Key threats include:

1. Ransomware: Cybercriminals encrypting healthcare data and demanding payment to restore access, causing operational disruption.
2. Hacking Attempts: Targeted efforts to breach healthcare systems for PHI theft or sabotage.
3. DDoS Attacks: Disrupting healthcare network access, delaying critical operations.
4. Exploitation of IoT/IoMT Vulnerabilities: Cyberattacks targeting medical devices or connected systems, endangering patient safety.
5. Phishing Attacks: External attempts to deceive employees into granting unauthorized access.
6. Third-Party Attacks: Compromising vendors or business associates with access to healthcare systems.

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

c. Vulnerabilities in current systems and processes

Many vulnerabilities stem from outdated or insufficiently secured systems and processes. These include:

1. Legacy Systems: Older software and hardware that lack the latest security patches.
2. Weak Authentication Measures: Reliance on single-factor authentication or shared credentials.
3. Insufficient Encryption: Sensitive data not properly encrypted in transit or at rest.
4. IoT/IoMT Weaknesses: Poorly secured connected medical devices susceptible to exploitation.
5. Lack of Training: Employees unaware of best practices for cybersecurity and HIPAA compliance.
6. Vendor Risks: Business associates with inadequate security controls exposing systems to breaches.
7. Limited Resources: Insufficient budgets or staffing to address critical cybersecurity needs.
8. Poor Patch Management: Delays in applying security updates to mitigate known vulnerabilities.
9. Incomplete Asset Inventories: Missing or outdated records of software and hardware assets, complicating security efforts.

Threat	Potential Impact	Mitigation Measures
Insider Threats	Unauthorized access to sensitive data	Logging, monitoring, and role-based permissions
Weak Encryption	Data leakage or interception during transfer	Implement AES-512 and TLS encryption
Ransomware	Data loss and system downtime	Regular backups, endpoint protection, and rapid recovery plans
Phishing	Unauthorized system access	Multi-factor authentication, user training, and phishing simulations
IoMT Vulnerabilities	Compromise of connected medical devices	Isolate IoMT networks, strengthen device security
Lack of Auditing	Unnoticed breaches or unauthorized changes	Comprehensive logging and periodic audits

Table synthesized from HC-C04107 Data summarizing threats and mitigation strategies

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

V. Access Control Policies

A. User/Subject Identification

a. User groups and roles based on HC policy

- Root: IT Director, Bioinformatics Director, System Administrator, Bioinformatics Supervisor.
- Bioinfo: Bioinformatics Director, Bioinformatics Supervisor.
- Bioinfoclin: Bioinformatics Director, Bioinformatics Supervisor.
- Clinical: Medical Directors, Clinical Staff.
- Research: Researchers, Laboratory Technicians.
- HLA: HLA Lab Technicians, Researchers.
- Smbgroup: System Administrator.

Subject/Role	Description
Root	System administrators have full access to all data classifications and resources for system configuration, maintenance, and recovery operations.
Bioinfo	Bioinformatics analysts with access to non-clinical software and configurations.
Bioinfoclin	Members of this group can access clinical data and modify clinical software as per operational requirements. These users are integral to patient care workflows and system functionality.
Clinical	Clinical staff with access to patient data for healthcare purposes.
Research	Members are permitted to access research datasets, provided the data complies with Institutional Review Board (IRB) approval processes. This group is restricted from accessing clinical pipelines or sensitive patient information.
HLA	Specialists handling HLA-specific data and pipelines for both research and clinical purposes.
Smbgroup	Instrumentation systems or users responsible for managing raw data from lab equipment.

B. Protected Resources/Objects

a. Critical data assets and systems

Object/Resource	Description
Clinical Databases	Databases containing patient clinical data, including sensitive ePHI.
Non-clinical Software	Tools and pipelines used for non-patient-specific data processing and analysis.
Research Data	De-identified datasets used for academic and research purposes.
HLA Pipelines	Specialized systems for processing human leukocyte antigen data.
Instrument Configuration Files	Configuration data required for laboratory equipment operation and calibration.
AWS Cloud Storage	Cloud-based storage where sensitive data (e.g., sequencing files, clinical data) is maintained.

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

Clinical Microarray Data	Data derived from clinical microarray tests, often sensitive and specific to patient care.
Logs and Audit Records	Logs capturing system activities, access events, and security incidents.
Backup Data	Archived copies of critical clinical and research data for recovery purposes.

Table adapted from HC-C04107 Data Policies to illustrate assets or data that are accessed, manipulated, or protected

C. Access Control Models

a. Discretionary Access Control (DAC) evaluation

Subject/Role	Object/Resource	Access Level	Purpose
Root	Logs and Audit Records	Read, Write, Execute	Oversight, monitoring, and incident response.
	AWS Cloud Storage	Full Access	Administration of storage resources.
	Clinical Databases	Full Access	Maintenance and emergency overrides.
	Non-clinical Software	Full Access	System updates and pipeline management.
Bioinfo	Non-clinical Software	Read, Modify	Pipeline testing and configuration.
	Clinical Databases	No Access	Restricted to non-clinical data only.
	Logs and Audit Records	No Access	Not required for role responsibilities.
Bioinfoclin	Clinical Databases	Read, Write	Process and analyze clinical data.
	Non-clinical Software	Read	Reference data tools.
	Logs and Audit Records	No Access	Not relevant to clinical operations.
Clinical	Clinical Databases	Read, Write	Access patient information for treatment.
	Logs and Audit Records	No Access	Not required for clinical duties.
	AWS Cloud Storage	No Access	Data access is mediated through software.
Research	Research Data	Read	Conduct academic research.
	Clinical Databases	No Access	Prohibited due to sensitivity of ePHI.
	Logs and Audit Records	No Access	Not relevant to research activities.
HLA	HLA Pipelines	Read, Write	Analyze HLA-specific data.
	Clinical Databases	Restricted (HLA-specific data only)	Access HLA-related patient data.
	Non-clinical Software	Read	Use tools related to HLA pipelines.
Smbgroup	Instrument Configuration Files	Read, Write	Ensure proper operation of lab instruments.
	AWS Cloud Storage	Restricted (instrument-specific data)	Manage raw data uploads from instruments.
	Clinical Databases	No Access	Not within the scope of instrumentation role.

Table adapted from HC report for subject-object permissions based on discretionary access

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

b. Mandatory Access Control (MAC) evaluation

i. Classifications (Objects)

Classifications categorize objects based on their sensitivity and need for protection.

Classification	Description
Top Secret	Critical ePHI, HLA pipelines, security configurations, full system backups.
Confidential	Research data, audit logs, and clinical software configurations.
Internal	Instrument-generated raw data and non-sensitive system metadata.
Unclassified	General software documentation and publicly accessible information.

ii. Clearance Levels (Subjects)

Clearance levels determine the sensitivity of information a subject is authorized to access.

Clearance Level	Applicable Roles	Scope
Top Secret	Root, Bioinformatics Director	Full access to all data and configurations.
Confidential	Bioinfoclin, Clinical Staff, HLA Specialists	Access to patient data and related tools.
Internal	Smbgroup, Lab Technicians	Limited access to raw data and systems.
Unclassified	Research Staff, General Users	Access to public and non-sensitive data.

iii. Access Matrix

Using predefined rules, the MAC Access Matrix maps clearances (subjects) to classifications (objects).

Object/Resource	Top Secret	Confidential	Internal	Unclassified
Clinical Databases	Full Access	Read/Write	No Access	No Access
HLA Pipelines	Full Access	Read/Write	No Access	No Access
Research Data	No Access	Read/Write	Read-Only	Read-Only
Instrument Configurations	Full Access	Read/Write	Read/Write	No Access
Logs and Audit Records	Full Access	Read	Read	No Access
Raw Instrument Data	No Access	No Access	Read/Write	No Access
General Software Documentation	Full Access	Read	Read	Read-Only
AWS Cloud Storage	Full Access	Read/Write	No Access	No Access

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

iv. Complete List of Users and Roles with Classifications

Role	Clearance	Permitted Actions	Justification
Root	Top Secret	Full Access	Admin-level responsibilities.
Bioinfo	Confidential	Read/Write Non-clinical Data	Analyze non-patient data.
Bioinfoclin	Confidential	Read/Write Clinical Data	Process clinical patient data.
Clinical Staff	Confidential	Read/Write Clinical Databases	Patient care and analysis.
Research Staff	Unclassified	Read-only Research Data	Academic or non-sensitive analysis.
Lab Technicians (Smbgroup)	Internal	Read/Write Instrument Data	Manage and operate lab equipment.
HLA Specialists	Confidential	Read/Write HLA Pipelines	Analyze patient-specific HLA data.
External Vendors/Auditors	Case-by-case basis	Read-only where necessary, Write on agreed data	External assessments (if applicable).

v. Rules for Enforcing MAC

1. Access Control Rule:
   A subject can access an object only if its clearance level is equal to or higher than the classification of the object.
   E.g., A user with "Confidential" clearance cannot access "Top Secret" data.
2. No Discretionary Changes:
   Users cannot modify access permissions for themselves or others.
   Access levels are defined by security policies and implemented by the system.
3. Separation of Roles:
   Subjects are limited to actions required for their role.
   E.g., research cannot execute actions on clinical data, even with higher clearance.
4. Read Down, Write Up Policy:
   Read Down: Subjects can read data classified at their clearance level or lower.
   Write Up: Subjects can write to objects classified at their clearance level or higher.

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

D. Proposed Access Structure

a. Role-based access control (RBAC) framework

i. Roles and Permissions

Each role has predefined permissions aligned with job responsibilities and organizational requirements.

Role	Description	Permissions
System Administrator	Full control of all systems, resources, and configurations.	Full Access to all systems and data.
Bioinfo Analyst	Analyzes non-clinical data and software pipelines.	Read/Write Non-clinical software and data.
Clinical Staff	Accesses and updates clinical data for patient care.	Read/Write Clinical Databases.
Researcher	Conducts research using de-identified data.	Read-only Research Data.
HLA Specialist	Manages HLA pipelines for clinical and research purposes.	Read/Write HLA Pipelines and Data.
Lab Technician	Manages and operates lab instruments.	Read/Write Instrument Configurations.
Auditor/External Vendor	Conducts audits or assessments as needed.	Read-only Audit Logs and Reports.

ii. Resource Permissions Matrix

This table maps roles to resources, ensuring a structured RBAC implementation.

Resource/Role	System Admin	Bioinfo Analyst	Clinical Staff	Researcher	HLA Specialist	Lab Technician	Auditor/Vendor
Clinical Databases	Full Access	No Access	Read/Write	No Access	Read/Write	No Access	No Access
HLA Pipelines	Full Access	No Access	No Access	No Access	Read/Write	No Access	No Access
Research Data	Full Access	Read-only	No Access	Read-only	No Access	No Access	No Access
Non-clinical Software	Full Access	Read/Write	No Access	No Access	Read-only	No Access	No Access
Instrument Configurations	Full Access	No Access	No Access	No Access	No Access	Read/Write	No Access
Logs and Audit Records	Full Access	No Access	No Access	No Access	No Access	No Access	Read-only

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

VI. Additional Security Requirements

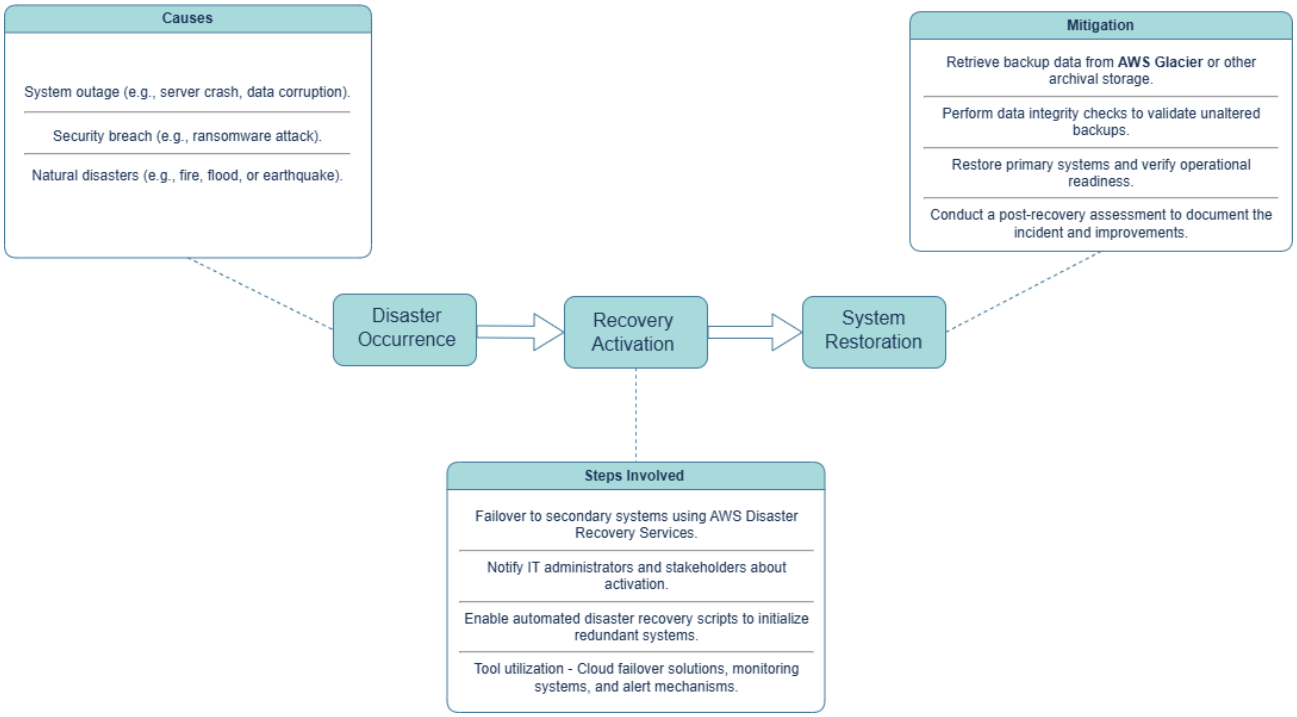
a. Availability measures & enhancements

To ensure the availability of critical electronic Protected Health Information (ePHI), HC must implement robust disaster recovery, emergency operations, and business continuity measures. These measures mitigate risks associated with system outages, data loss, and natural or technical disruptions.

1. Disaster Recovery:
   - Leverage AWS Disaster Recovery Services for fast failover to secondary systems, ensuring minimal downtime in the event of system failures.
   - Conduct bi-annual disaster recovery tests to validate the effectiveness and reliability of recovery processes.
   - Develop a comprehensive disaster recovery playbook that outlines steps for restoring operations within a defined Recovery Time Objective (RTO).
2. Emergency Operations:
   - Assign and train specific personnel to maintain critical clinical systems during outages. These roles ensure system accessibility for urgent healthcare operations.
   - Document and implement secure processes for accessing backup data stored in AWS Glacier during emergencies, ensuring compliance with HIPAA requirements.
3. Business Continuity:
   - Deploy redundant systems across multiple cloud regions to minimize risks from localized disruptions. For example, mirror critical systems between geographically distinct AWS data centers.
   - Schedule regular integrity checks on backup data to verify that it remains unaltered and accessible. Use automated tools for data validation to streamline this process.
   - Load balancing and scalable infrastructure to handle peak usage periods
   - Regular system maintenance and updates to prevent downtime due to technical issues

These measures ensure the availability of critical ePHI during system disruptions, aligning with HIPAA requirements and enhancing operational resilience.

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026



Disaster recovery workflow diagram

b. Data integrity controls

To maintain the accuracy and consistency of healthcare data throughout its lifecycle, the following controls should be put in place:

- Input validation checks to ensure data accuracy at the point of entry
- Data encryption both in transit and at rest to prevent unauthorized modifications
  - AES-512 for robust data encryption.
  - Transport Layer Security (TLS) as a replacement for Secure Socket Layer (SSL).
- Regular data reconciliation and validation processes to identify and correct discrepancies
- Hash Verification: Implement hash-based checks for all data transfers to confirm the integrity of files during transmission.
- Regular Validation: Conduct periodic integrity checks on archived data to detect unauthorized changes or corruption.
- Version control and audit trails to track changes made to critical data

c. Audit and monitoring capabilities

Implementing comprehensive audit and monitoring capabilities is crucial for maintaining security and compliance:

1. Automated Logging: Use AWS CloudTrail to collect detailed logs of system access and data modifications.
2. Secure Retention: Retain logs securely for future investigations or audits.
3. Alert Mechanisms: Configure alerts to notify system administrators immediately of unauthorized data modifications or suspicious activities.

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

4. To safeguard data integrity, audit logs will track all system activities. Any unauthorized data modification attempts will trigger immediate alerts to the system administrator
5. Amazon GuardDuty: Deploy for real-time monitoring of network traffic and user activities, detecting anomalies and potential threats.
6. Compliance Monitoring Tools: Continuously monitor for HIPAA compliance, ensuring adherence to regulatory requirements and organizational policies.
7. Regular Audits: Schedule periodic security audits to identify weaknesses and verify the effectiveness of implemented controls.
8. Vulnerability Assessments: Use automated tools to detect and address system vulnerabilities.
9. Periodic review of audit logs and reports by security personnel to identify suspicious patterns or anomalies

By combining robust data integrity controls, automated audit mechanisms, and real-time monitoring, HC ensures the accuracy, security, and compliance of its healthcare data. Advanced tools like AWS CloudTrail and Amazon GuardDuty enhance the organization's ability to detect, prevent, and respond to potential threats, safeguarding critical ePHI.

VII. Gap Analysis

b. Threat areas not fully addressed by access control policies

Based on the review of HC policies and NIST guidelines, several threat areas are not fully addressed by the current access control policies:

1. Insider threats: While HC has defined user groups and roles, there is insufficient focus on monitoring and mitigating insider threats, whether intentional or accidental.
2. Mobile data access: The HC policies do not specifically address the security risks associated with mobile access to clinical data and systems.
3. Third-party risk management: There is a lack of comprehensive policies for managing and monitoring the cybersecurity of third-party vendors and service providers.
4. IoMT (Internet of Medical Things) security: The policies do not adequately address the security challenges posed by connected medical devices and IoT technologies in the healthcare environment.
5. Web application security: There is insufficient detail on securing web-based services like patient portals and other online applications.
6. Incident response and disaster recovery: While mentioned, the HC policies lack comprehensive incident response and disaster recovery procedures.

c. Assessment of residual risks

After implementing the current access control policies, several residual risks remain:

1. Human error: Despite access controls, there is still a risk of employees inadvertently compromising data security through phishing attacks or social engineering tactics.
2. Privilege escalation: There is a residual risk of users gaining unauthorized elevated access due to potential misconfigurations in access control settings.
3. Data encryption gaps: While data transfer protocols are encrypted, there may be gaps in encryption for data at rest, particularly in legacy systems or temporary storage locations.
4. Emerging technologies: As new technologies are adopted, there is a risk that access control policies may not keep pace with the evolving threat landscape.
5. Compliance gaps: There may be residual risks related to incomplete implementation of all HIPAA Security Rule requirements, particularly in areas not fully addressed by current policies.

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

6. Third-party vulnerabilities: Despite contractual obligations, there remains a risk that third-party vendors may not maintain the same level of security standards, potentially exposing the organization to breaches.
7. Delayed threat detection: Without comprehensive monitoring and auditing processes, there is a risk that unauthorized access or data breaches may go undetected for extended periods.
8. Ransomware and advanced persistent threats: Current access control policies may not fully mitigate the risks posed by sophisticated ransomware attacks or long-term, stealthy intrusions.

To address these residual risks, the organization should consider implementing additional security measures, enhancing employee training programs, and regularly updating policies to address emerging threats and technologies.

VIII. Recommended Additional Controls

a. Administrative controls

1. Have an enhanced security awareness training program:
   - Topics: HIPAA requirements, phishing awareness, incident reporting
   - Frequency: Quarterly refreshers with mandatory completion.
2. Develop comprehensive incident response plan:
   - Create detailed procedures for identifying, containing, and mitigating security incidents
   - Establish a dedicated incident response team with clearly defined roles
3. Implement formal risk assessment process:
   - Methodology: NIST SP 800-66 Appendix E guidelines.
   - Frequency: Annually or after significant system changes.
4. Strengthen third-party vendor management:
   - Implement a vendor risk assessment program
   - Regularly audit third-party compliance with security requirements
5. Enhance policy documentation:
   - Create detailed policies for areas not currently addressed, such as mobile device usage and IoMT security
   - Regularly review and update all security policies

b. Physical controls

1. Enhance physical access controls:
   - Implement multi-factor authentication/biometrics for server room access
   - Install security cameras (CCTV) in sensitive areas
   - Increase surveillance retention to 90 days.
2. Improve environmental controls:
   - Upgrade fire suppression systems in server rooms
   - Implement redundant power supplies and cooling systems
3. Strengthen asset management:
   - Maintain an up-to-date inventory of all hardware and software assets
   - Implement asset tagging and tracking for all devices containing sensitive data
4. Secure disposal procedures:
   - Implement secure methods for disposing of physical media containing sensitive data
   - Establish a chain of custody for assets being decommissioned

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

c. Technical controls

1. Implement advanced access controls:
    - Deploy a robust Identity and Access Management (IAM) system
    - Implement multi-factor authentication for all user accounts
2. Enhance network security:
    - Deploy next-generation firewalls and intrusion detection/prevention systems
    - Implement network segmentation to isolate critical systems and data
3. Improve data encryption:
    - Use FIPS-compliant methods for all stored and transmitted data.
    - Require TLS 1.2+ for all network communications.
4. Deploy advanced endpoint protection:
    - Implement endpoint detection and response (EDR) solutions on all devices
    - Deploy mobile device management (MDM) for all company-owned and BYOD devices
5. Enhance monitoring and logging:
    - Implement a Security Information and Event Management (SIEM) system
    - Set up real-time alerts for suspicious activities and potential security breaches
6. Strengthen patch management:
    - Implement an automated patch management system
    - Establish procedures for timely patching of all systems and applications
7. Implement data loss prevention (DLP):
    - Deploy DLP solutions to prevent unauthorized data exfiltration
    - Set up content-aware policies to detect and prevent sensitive data leaks
8. Enhance backup and recovery:
    - Implement a 3-2-1 backup strategy (3 copies, 2 different media, 1 off-site)
    - Regularly test data restoration procedures to ensure effectiveness

IX. Implementation Roadmap

a. Prioritized list of recommended actions

1. Conduct a comprehensive risk assessment
    - Identify and document all systems containing EPHI
    - Evaluate current security controls and gaps
    - Determine risk levels for identified vulnerabilities
2. Develop and implement a formal risk management program
    - Establish a risk management committee
    - Create policies and procedures for ongoing risk assessment and mitigation
3. Enhance access control measures
    - Deploy multi-factor authentication for all user accounts
    - Review and update user access rights regularly
4. Strengthen data encryption
    - Implement end-to-end encryption for data in transit and at rest
    - Update encryption algorithms to current standards
5. Improve security awareness and training
    - Develop role-specific security training programs
    - Conduct regular phishing simulations and security drills
6. Implement comprehensive logging and monitoring
    - Deploy a Security Information and Event Management (SIEM) system

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

- Establish procedures for regular log review and incident response

7. Enhance business associate management
   - Review and update all business associate agreements
   - Implement a vendor risk assessment program
8. Develop and test a comprehensive disaster recovery plan
   - Create detailed procedures for various disaster scenarios
   - Conduct regular disaster recovery drills
9. Implement advanced endpoint protection
   - Deploy endpoint detection and response (EDR) solutions
   - Implement mobile device management (MDM) for all devices
10. Establish a formal security evaluation process
    - Conduct regular internal security audits
    - Engage third-party auditors for independent assessments

b. Estimated timelines and resource requirements

1. Short-term (0-6 months):
   - Risk assessment: 2-3 months; requires dedicated risk assessment team or external consultant
   - Security awareness training: Ongoing; requires training development and delivery resources
   - Access control enhancements: 3-4 months; requires IT staff and potential software/hardware investments
2. Medium-term (6-12 months):
   - Encryption improvements: 4-6 months; requires IT security specialists and potential software/hardware upgrades
   - SIEM implementation: 6-8 months; requires significant IT resources and budget for SIEM solution
   - Business associate management: Ongoing; requires legal and procurement team involvement
3. Long-term (12-18 months):
   - Comprehensive disaster recovery planning: 6-8 months; requires cross-departmental involvement and potential infrastructure investments
   - Advanced endpoint protection: 8-10 months; requires IT security team and budget for EDR/MDM solutions
   - Formal security evaluation process: Ongoing; requires dedicated internal audit team and budget for external auditors

Resource requirements:

- Dedicated information security team, including HIPAA Security Officer
- IT infrastructure upgrades (hardware and software)
- Budget for security tools and solutions (e.g., SIEM, encryption, EDR)
- Training resources for staff awareness programs
- Legal and compliance expertise for policy development and business associate management
- Potential external consultants for specialized assessments and implementations

Kamalesh Jayapandiaraj Arumugam
karumuga@usc.edu
M.S in Cybersecurity, May 2026

X. Conclusion

The HIPAA Security Rule establishes critical requirements for protecting electronic protected health information (EPHI) in healthcare organizations. Through this analysis of the Hospital Center's (HC) policies and NIST guidelines, several key conclusions can be drawn:

1. HC has implemented many important security measures aligned with HIPAA requirements, including access controls, data encryption, and de-identification procedures. However, some gaps remain in areas like formal risk assessment and comprehensive incident response planning.
2. Adopting a structured approach like NIST's Risk Management Framework can help HC systematically address HIPAA compliance and overall cybersecurity. This includes conducting regular risk assessments, implementing appropriate controls, and continuously monitoring their effectiveness.
3. Enhancing access control policies through role-based access control (RBAC) and mandatory access control (MAC) models can provide more granular and robust protection of EPHI.
4. Additional focus is needed on emerging threat areas like mobile device security, IoT/medical device vulnerabilities, and third-party risk management to comprehensively protect EPHI.
5. Ongoing security awareness training and fostering a culture of compliance are critical for mitigating insider threats and ensuring proper handling of sensitive data.
6. Regular security audits, both internal and external, are essential to identify vulnerabilities, assess policy effectiveness, and maintain HIPAA compliance over time.

By addressing the identified gaps and implementing the recommended additional controls, HC can significantly strengthen its HIPAA compliance posture and overall cybersecurity program. This will not only help meet regulatory requirements but also enhance patient trust and the organization's ability to protect critical health information in an evolving threat landscape.

XI. References

- NIST SP 800-66 Compliance guide from Prevalent
- MedTrainer blog post on HIPAA compliance for healthcare facilities
- NIST announcement on publication of SP 800-66 Revision 2
- HIPAA Journal article on HIPAA compliance for hospitals
- Kiteworks guide on HIPAA compliance requirements and checklist
- Prevalent blog post on NIST 800-66 and HIPAA Security Rule compliance