DSCI 519 - Foundations and Policy for Information Security Project

Rishit Saiya (rsaiya@usc.edu)

1. Introduction

A bioinformatics business called "The Center" focuses on research, molecular pathology, and clinical genetics labs. Utilizing technology to handle and analyze biological data is the primary purpose of the bioinformatics field. It contains several stages, including ones for biological data analysis and storage. The Center has an agreement with a different business called Cartagenia that gives it access to a clinical informatics platform for performing data analysis. Despite the fact that Cartagenia conducts data analysis, The Center alone retains ownership of the data, and Cartagenia will only serve as a data processor. The Center's data is maintained by Amazon Web Services, a cloud service provider (AWS). With the help of its numerous storage and processing services, such as EC2, S3, and Glacier, AWS keeps its servers and storage in the cloud that are HIPAA compliant [1].

The Health Insurance Portability and Accountability Act (HIPAA) [5] was created to regulate how "covered entities" (such as health insurers and medical service providers) and other businesses that may acquire such information, collect, disclose, and preserve customers' protected health information (PHI). HIPAA is relevant to the business since "The Center" deals with protected health information (PHI) and electronically protected health information (ePHI). Company must adhere to HIPAA rules' policies and controls. The documents outline data policies, including the steps the Center takes to protect the privacy and security of its clients' and patients' personal information on both a process and product level. It also outlines the data retention policy for all cytogenetic, clinical microarray, and next generation sequencing data created inside the Center, as well as procedures for sharing, storing, and transferring next generation sequencing (NGS) data that is generated, processed, and reported.

2. Protection Policies for The Center's Information

2.1 Database Policy

The implementation of this regulation is necessary to impose restrictions on databases. It has to be encrypted using a certain cryptographic method, such as AES 256, etc. ACL should also be kept up to date for DBAs (Database Administrators).

2.2 Policies for Data Security and Confidentiality

The confidentiality of data and information systems that "The Center" holds are the major emphasis of this policy. It contains several sub-policies that have the same objective. This policy must be consistent with the hospital's broader guidelines. If the hospital center's IT director is unavailable, the bioinformatics director must make the necessary choices about data security and confidentiality [7].

2.2.1 Access Control Policy

This policy identifies the individuals with the power to give access to resources. Access is granted subject to a number of conditions, such as infrastructure type, user groups, integration, roles, and environments. For instance, the hospital's IT department manages the username and passwords for any equipment that is connected with the LDAP configuration of the facility, albeit the IT Director or a designee may authorize access. The IT Director, the Bioinformatics Director, or a representative of each of them must provide root access. Similar to this, several user roles are specified together with their access rights to resources. For instance, the Bioinfoclin group is only allowed to see clinical data and other related information.

2.3 Log Management Policy

It gives instructions on the kinds of logs that must be kept and their criteria. It also details the folders in which logs will be kept. For example, user names and access privileges must be recorded in the computing equipment access log (FORM.HC-40101.1), whereas maintenance related logs (such as network cards and OS upgrades) must be recorded in the computing equipment maintenance log (FORM.HC-C04101.2) [4].

2.4 Security Policy

It outlines the safeguards that must be put in place to protect the information systems and data that HC holds. Controls for network access and physical access are included.

2.4.1 Physical Access Policy

It is made up of checks that must be used to carry out the physical access policy. Only the Director of Bioinformatics, Directors' designees, IT staff, and pre-approved/authorized suppliers have physical access to the IDF/HC server. Three biometric security mechanisms are in place at USC HPCC and are used whenever someone tries to access gear.

2.4.2 Network Access Policy

It describes the precautions that must be taken when logging onto the network. These protections are dependent on a number of elements that are taken into account. For instance, unless VPN access is permitted, a hospital's network may only be accessed when onsite. The Director of Bioinformatics or his designee is the only person with network access at USC HPCC. Furthermore, there are no connections to the dark web.

2.5 Policy of Acceptable Usage

It describes the rules that users must abide by when accessing data and information systems. It states that in order to avoid unauthorized access to protected data, users must not share their login information with any other users and must log out of all systems when not in use. Additionally, it states that any electronic correspondence must use the hospital's email address. Personal email addresses are not permitted. Additionally, it states that all users who have access to clinical data must complete HIPAA training in accordance with the requirements and specifications established by the institution.

2.6 Policy for Third Party Security

Because Cartagenia and other third parties, such AWS, conduct some processes, it is crucial. There should be a suitable agreement in place that includes terms relating to confidentiality, security, the ability to audit, and nondisclosure agreements (Non-Disclosure Agreement). BAA (Business Associate Agreement) in place with AWS in this instance.

2.7 Data Transfer Policy (When data is in motion/migration)

It is a comprehensive policy that contains restrictions on data collection, transfer, transmission, identifiers, and de-identifiers, among other things. According to the documentation, the different types of such namely cytogenic, NGS or maybe even the cytogenic data is all generated within the organization [6]. However, the clinical reports maybe a subset of the patient record, but apart from that no information about Clinical NGS Testing is shared to outside reference labs or other service providers. A checksum is included with every data file to guarantee that it is transferred in its whole and is not damaged.

2.7.1 Backup Policy

It specifies the checkpoints that must be put in place for data backup. Along with the frequency of backups, it iterates over the different types of data that need to be saved. RAID solutions, integrity standards to be upheld by MD5, CRC32, backup tapes, TSM server, and appropriate scheduling are all included.

2.7.2 Data Access Policy

This policy specifies the rules that must be adhered to while accessing data. The transfer of data generated at the Clinical end created within The Center to personal external drives or clouds like Dropbox, Google Drive is expressly forbidden, according to the statement.

2.7.3 Data Transmission Policy

The controls listed in this policy must be adhered to while transmitting data. It claims that opposing cryptographic techniques are used to secure data transported outside of the network. Furthermore, only 2 ways are permitted for data transmission to AWS. Through the AWS Snowball Appliance Service or over the internet using an encrypted storage device. Further instructions are provided on how to connect to Cartagenia BENCHLab NGS and transfer data.

2.7.4 De-Identification Policy

When dealing with HIPAA compliance, De-Identification is crucial. The standards and procedures that must be followed for de-identification are laid out in this policy. Samples are de-identified and given a sample identification in accordance with policy and file naming standard.

2.7.5 Encryption Policy
It is among the most significant protective measures. This policy outlines the information encryption standards that must be followed. It advises using SSH to connect to distant servers. To ensure data confidentiality and integrity, HTTPS and other comparable cryptographic technologies should be employed.

2.8 Policy for Data Retention
Data compromise might occur if data is not stored securely. Controls for data protection must be put in place for various degrees of data retention. It addresses issues including data storage, data retention time, backup strategy, and more.

2.8.1 Data Recovery
From the perspective of the security component of availability, this strategy is absolutely essential. It contains information about the people qualified to carry out data recovery procedures. The circumstances/situations that can cause data recovery are also described. If data becomes damaged during processing or analysis, data recovery can still be done.

2.8.2 Storage Policy
This policy outlines the storage criteria that must be adhered to in order to prevent data loss or compromise. One of the main points of this policy is that all the raw and processed data produced on instruments and equipment provided by the vendor must be duplicated or relocated to a local repository for short-term storage and/or further processing and analysis.

3. Threat Space

3.1 Backdoor
Companies, including The Center, should take this issue seriously since it gives hostile actors unrestricted access to resources that might have severe effects. Unauthorized users and malevolent users can circumvent security measures in this danger in order to access system resources. Malicious parties can get data about the systems installed in HC through backdoors. Additionally, it has the ability to track user activity and data that may be shared with C2C servers, potentially disclosing private information at a high cost to HC.

3.2 Cloud Threats
Because this configuration uses AWS cloud services, HC and Cartagenia must exercise due vigilance in light of the rising number of cyberthreats. Although AWS cloud services are thought to be safe, appropriate precautions must be taken to ward off dangers. Both the obligations of the cloud service provider and the cloud user should be clearly stated. For these threats to be effectively dealt with, both parties must exercise caution as they carry out their respective portions of the operations. Improper configuration takes the form of information systems at HC not being hardened as per controls outlined in HC's policies and procedures. As a result, threat actors may find a way to breach the systems and access the sensitive health data that HC is in possession of.

3.3 Lack of Encryption
When it comes to adhering to HIPAA rules, encryption is a crucial element. Any organization, including HC, has major difficulties due to weak cryptography suites. Malicious actors may compromise the security and privacy of sensitive health data if data flow between The Center and Cartagenia via the BENCHLab platform is not protected by a strong cryptographic solution. Similar to this, improper data encryption in databases and storage might allow for bad actors to leverage it to their advantage and compromise The Center's data's integrity.

3.4 Ransomware
The healthcare sector, including cover businesses, is vulnerable to the danger of ransomware. The Center and other bioinformatics businesses are not an exception. The frequency of ransomware assaults over the last few years is one way it has been demonstrated. If this danger materializes, it might paralyze all activities by encrypting resources (files) and blocking access to them. Resources can only be accessed by paying a ransom to hostile actors, which occasionally does not work. Malicious actors occasionally steal this material and publish it on open networks. As a result, it may also affect privacy, secrecy, and availability. The entire system can be

affected in a matter of minutes. Access to or disclosure of HC data might have serious consequences and would be a flagrant breach of HIPAA rules. Attacks using ransomware might take the form of phishing emails, infected USB drives, malicious downloads, password compromises, malicious file attachments, etc.

3.5 Malware

It is described as software that is purposefully created to harm networks, information systems, etc. Malicious software has a large aim. Malwares are a general term for all types of harmful software. This contains spyware, Trojan horses, worms, and viruses. Sensitive data may be improperly divulged and HC's systems may be breached if safeguards at various tiers are not correctly enforced. Numerous malwares that propagate by lateral movement have the ability to affect several computers that are connected to the infected one. The Center (HC), Cartagenia must thus have appropriate controls in place for all of its systems.

3.6 Man in the Middle Attack

As the set-up in question involves three different companies (HC, Cartagenia, and AWS), data communication between them is necessary. Communication between the parties engaged in this setup may be vulnerable to a Man in the Middle attack if it is not done securely. To address this problem, a strong PKI solution or any comparable mechanism should be in place.

3.7 Physical Threats

Threats from the physical world are at least as hazardous as those from the technical internet. It may potentially halt all corporate activities. Physical dangers include, but are not limited to, earthquake, flood, fire, and system theft. There are many different types of physical hazards. There must be a disaster recovery [3] center or a center close to one in addition to proper physical and environmental controls. DR is mentioned in the documentation provided for AWS, but it should also be taken into account for HC and Cartagenia.

3.8 Procedural/Legal Threats

An appropriate agreement, similar to the one between Cartagenia and AWS, must exist between HC and Cartagenia. NDA (Non-Disclosure Agreement), right to audit, confidentiality clause, third party security provision, etc. should all be included in the contract. Without such an agreement, there will be a considerable risk that HC won't be able to enforce the rules and regulations that it wants Cartagenia to go by.

3.9 Weak Authentication

If robust authentication procedures are not used, HC will be in danger. There are several types of authentication controls, such as VPN tokens, smartcards, biometric controls, and passwords. The ones that are used most frequently are passwords. Sensitive health information held by HC may be accessed, modified, or altered without authorization if the password is weak or simple to guess. The BENCHLab platform uses credentials in a similar way to upload data to Cartagenia. If multi-factor authentication is not used or credentials are not sufficiently strong, there is a high likelihood that malicious actors will engage in unauthorized activities.

3.10 Trojan Horse

It is a specific type of malware that poses as legitimate software and conceals its dangerous nature in order to deceive users into believing it to be a real and safe file. Trojan horses come in a variety of varieties, including exploit Trojans, rootkit Trojans, banker Trojans, DDoS Trojans, and downloader Trojans, among others. If the restrictions outlined in HC policies and procedures are not carefully followed, the Center might become a victim of this danger. This danger may be delivered by email phishing scams or download upgrades. It might remove, obstruct, change, or otherwise negatively affect data, as well as impair the functionality of HC's information systems.

3.11 Social Engineering Attack

These are the kind of assaults that lure people into doing something they shouldn't. Attackers can obtain sensitive information about HC, including health information, login passwords, and other sensitive data, using these methods. One of the best instances is phishing, when attackers pretend to be well-known people or organizations in order to deceive consumers into clicking URLs or divulging private information. Employees at HC might become victims of these assaults if there is a control breach and they are not well trained, which will have major repercussions.

3.12 Improper Authorization

In order to prevent principals or subjects from obtaining access privileges they are not meant to have, authorization entails defining and tightly enforcing appropriate access permissions. Inaccurate implementation in HC or Cartagenia might lead to the unauthorized exposure of private medical information. One of these problems that HC must address is authorization misuse.

4. Access Control Policies

From a DAC standpoint, the decision of whether the subject can access the object is made by the data owner. The HC IT director or the Bioinformatics director will choose the users' access privileges in the hypothetical situation. Whether or whether the user may access the item. Subject levels are modified, it is assumed. In order to get the access policy specified by the document, confidentiality and integrity levels are defined [11].

4.1 Subjects

The objects and subjects are mentioned in Table 1.

Objects	Subjects
Clinical Data HLA Data Non-Clinical Data Raw Data Research Data	Bioinfo Bioinfoclin Clinical HLA Research Root SMBGroup

Table 1: List of Objects and Subjects

4.2 Levels and Categories

The levels and categories are as mentioned in Table 2.

5. Access Class and MAC Labels

The level of confidentiality is assumed as Internal < Confidential < Restricted. The BLP Policy [8] for Confidentiality/Security follows the No Read Up, No Write Down and BIBA Policy for Integrity follows the No Read Down, No Write Up [10]. The access classes and MAC Labels defined for The Center in this system are as follows:

Levels	Categories
Internal (I) Confidential (C) Restricted (R)	Clinical Information (CI) HLA Information (HI) Non-Clinical Information (NCI) Raw Information (RI) Research Information (REI)

Table 2: List of Levels and Categories

5.1 Confidential

In here Confidential is referred to C:
(C, {NCI,HI,REI,RI}) | (C, {NCI,HI,REI}), (C, {NCI,REI,RI}), (C, {NCI,HI,RI}), (C, {HI,REI,RI}) | (C, {NCI,HI}), (C, {NCI,REI}), (C, {NCI,RI}), (C, {HI,REI}), (C, {HI,RI}), (C, {REI,RI}) | (C, {NCI}), (C, {HI}), (C, {REI}), (C, {RI})

5.2 Internal

In here Internal is referred to I:
(I, {RI,NCI}) | (I, {RI}), (I, {NCI})

5.3 Restricted

In here Restricted is referred to R:
(R, {NCI,RI,CI,NEI,HI}) | (R, {NCI,RI,CI,REI}), (R, {NCI,RI,CI,HI}), (R, {NCI,CI,REI,HI}), (R, {NCI,RI,REI,HI}), (R, {RI,CI,REI,HI}) | (R, {NCI,RI,CI}), (R, {NCI,RI,REI}), (R, {NCI,RI,HI}), (R, {NCI,CI,REI}), (R, {NCI,CI,HI}), (R, {NCI,REI,HI}), (R, {RI,CI,REI}), (R, {RI,CI,HI}), (R, {RI,REI,HI}), (R, {CI,REI,HI}) | (R, {NCI,RI}), (R, {NCI,CI}), (R, {NCI,REI}), (R, {NCI,HI}), (R, {RI,CI}), (R, {RI,REI}), (R, {RI,HI}), (R, {CI,REI}), (R, {CI,HI}), (R, {REI,HI}) (R, {NCI}), (R, {RI}), (R, {CI}), (R, {REI}), (R, {HI})

5.4 Subjects and their corresponding Labels
Root: (R, {CI,NCI,RI,REI,HI}), (R, {CI}), (C, {NCI}), (C, {REI}), (C, {HI, REI}), (I, {RI}) | Bioinfo: (C, {NCI}) | BioInfoclin: (R, {CI}) | Clinical: (R, {CI}) | HLA: (C, {HI,REI}) | Research: (C, {REI, HI,RI}), (C, {REI}) | SMBGroup: (I, {RI})

5.5 Objects and their corresponding Integrity Labels
Clinical Data: (R, {ICI}) | HLA Data: (C, {IHI,IREI}) | Non Clinical Data: (C, {INCI}) | Raw Data: (I, {IRI})
Research Data: (C, {IREI}), (C, {IHI,IREI})

5.6 Subjects and their corresponding Integrity Labels
Root : (R, {ICI}), (C, {INCI}), (C,{IREI}), (C, {IHI, IREI}),(R, {ICI,INCI,IRI,IREI,IHI}), (I, {IRI})
Bioinfo: (C, {INCI}) | Bioinfoclin: (R, {ICI}) | Clinical: (R, {ICI}) | Research: (C, {IREI, IHI}), (C, {IREI})
HLA: (C, {IREI,IHI}) | SMBGroup: (I, {IRI})

6. Substantiation of Label Assignments to Subjects
The nomenclature used in the following subsection's heading would be as (Subject-Associated Object with it). The rights of Read and Write are denoted as 'r' and 'w' here respectively [9].

6.1 Bioinfo - Non-Clinical Data
The security level for Bioinfo is (Confidential, {NCI}), whereas the security level for Nonclinical Data is (Confidential, {NCI}). Here, Bioinfo is capable of both (r, w) access rights and Non-Clinical Data. Similar to Bioinfo, Non-Clinical data also has an integrity level of (Confidential, {INCI}). Once more, Bioinfo has the ability with access rights: (r, w) Non-Clinical data. (r, w) access rights will be the intersection of the two. Bioinfo job holders have the access right to (r, w) to Non-Clinical Data. Bioinfoclin's integrity level is (R, {INCI}), and the same is true for Clinical Data. Once more, Bioinfoclin has the access rights of (r, w) to Clinical Data. Access Rights of (r, w) will be the intersection of the two. Subjects with the Bioinfoclin role have access to and the ability to edit Clinical Data. The procedure is the same for a Clinical subject in terms of (r, w) access rights to Clinical Data.

6.2 Root - Raw Data
Raw Data's security level is (I, {RI}), as is Root's security level. Because all levels are equal, the subject is able to read and write to raw data. So, (r, w) are the access privileges. The security level of Raw data is also (I, {IRI}), as is the integrity level of Root. Again, both read and write operations are possible since the two integrity levels are the identical. The access permissions will thus be (r, w) and (r, w) will also apply to the intersection of the two. This conforms to the principles of HC. Similarly, Root subject has access to and control of HLA, Non-Clinical, Clinical, and Research Data. However, in order to access or alter all of these items, subject level must be changed

6.3 HLA - Research Data
The security level for the HLA subject in this instance is (C, {HI,REI}), while the security level for the research data is (C, {REI}). The subject here overpowers the object. HLA can therefore read research data. The subject's integrity level is (C, {IREI,IHI}), and the integrity level of the study data is (C, {IREI,IHI}) as well. To gather information, the subject can (r, w). Only (r) will be at the intersection of (r, w) and (r). HLA individuals may thus read research data.

6.4 HLA - HLA Data
The security level for HLA subjects is (C, {HI,REI}), while the security level for HLA data is (C, {HI,REI}). As a result, the individual is able to read and write HLA data. The integrity level for the subject is (C,

{IREI,IHI}), while the integrity level for the HLA data is (C, {IREI,IHI}). The subject can (r, w) HLA data effectively. (r, w) also describes the intersection of the two. Therefore, HLA subjects are able to read and write HLA data.

6.5 Research - HLA Data

In this instance, the security level for the Research subject is (C, {REI, HI, RI}) while the security level for the HLA data is (C, {IHI,IRE}). As a result, the topic here overpowers the object. Therefore, the subject is limited to reading items. The subject's integrity level is (C, {IREI}), and the integrity level of the HLA Data is (C, {IREI}) as well. In this instance, the subject may both read from and write to the object. There will be a (r) only access sign at the intersection of (r, w). Therefore, eventually study participants can only read data

6.6 SMBGroup - Raw Data

Security roles for SMBgroup and Raw data are (I, {RI}) and (I, {RI}), respectively. As a result, the subject is able to read and write data from Raw. In terms of integrity level, Raw Data's security function is Internal (RI) and the subject's integrity level is (I, {IRI). SMBGroup can therefore read and write Raw data. both intersect, which is (r, w). SMBGroup is therefore able to read from and write to Raw data.

6.7 Research - Research Data

Research is (C, {REI}) secure, and research data is (C, {REI}) secure. As a result, study participants can access research data. The study subject's integrity level is (C, {IREI}), while the integrity level of the research's data is (C, {IREI}). Therefore, study participants can (r, w) gather data. Both will intersect at (r, w), allowing subjects to (r, w) research data.

7. Access Control Matrix

The conventional notation of Read and Write - (r, w) access rights is used in Table 3.

Subjects/ Objects	Clinical Data	HLA Data	Non-Clinical Data	Raw Data	Research Data
Root	r, w	r, w	r, w	r, w	r, w
Bioinfo	r, w				
Bioinfoclin	r, w				
Clinical	r, w				
HLA	r, w	r			
Research	r	r, w			
SMBGroup	r, w				

Table 3: Access Control Matrix for the defined subjects across the objects

This Access matrix is consistent with the access control policies listed in the Data Policies, which state that the Bioinfo group can (r, w) Non-Clinical Data, the Bioinfoclin group can (r, w) Clinical Data, the Clinical group can (r, w) Clinical data, the Research group can (r, w) Research Data, the Research group can (r, w) HLA Data, the SMBGroup can (r, w) Raw Data.

8. Capability Lists

The capability lists for the above-mentioned subjects are as follows:

8.1 Root

The capability lists for the subject Root is as follows:

Subjects/ Objects	Clinical Data	HLA Data	Non-Clinical Data	Raw Data	Research Data
Root	r, w	r, w	r, w	r, w	r, w

Table 4: Capability List – Root

8.2 Bioinfo

The capability lists for the subject Bioinfo is as follows:

Subjects/ Objects	Clinical Data	HLA Data	Non-Clinical Data	Raw Data	Research Data
Bioinfo	r, w				

Table 5: Capability List – Bioinfo

8.3 Bioinfoclin

The capability lists for the subject Bioinfoclin is as follows:

Subjects/ Objects	Clinical Data	HLA Data	Non-Clinical Data	Raw Data	Research Data
Bioinfoclin	r, w				

Table 6: Capability List – Bioinfoclin

8.4 Clinical

The capability lists for the subject Clinical is as follows:

Subjects/ Objects	Clinical Data	HLA Data	Non-Clinical Data	Raw Data	Research Data
Clinical	r, w				

Table 7: Capability List – Clinical

8.5 HLA

The capability lists for the subject HLA is as follows:

Subjects/ Objects	Clinical Data	HLA Data	Non-Clinical Data	Raw Data	Research Data
HLA	r, w	r			

Table 8: Capability List – HLA

8.6 Research

The capability lists for the subject Research is as follows:

Subjects/ Objects	Clinical Data	HLA Data	Non-Clinical Data	Raw Data	Research Data
Research	r	r, w			

Table 9: Capability List – Research

8.7 SMBGroup

The capability lists for the subject SMBGroup is as follows:

Subjects/ Objects	Clinical Data	HLA Data	Non-Clinical Data	Raw Data	Research Data
SMBGroup	r, w				

Table 10: Capability List - SMBGroup

9. Potential Enhancements

There are few security aspects (availability) and few risks that these rules cannot handle, despite the fact that access control policies incorporate measures that address multiple elements of security (confidentiality and integrity) and diverse threats. The availability element is influenced if confidentiality and integrity are implemented strictly.

When it comes to a few dangers, these policies are highly successful. One of the threats that Trojan horses can efficiently manage. As the secrecy policy is being applied (via BLP) in this case, the Trojan horse may be effectively dealt with. It is prohibited by the *- property, making write down impossible. Therefore, Trojan horse cannot damage data whose sensitivity is lower than that of the infected data (subject, etc.). Therefore, in this instance, a Trojan horse cannot alter fewer sensitive data, such as raw or non-clinical data. Additionally, if we take Strict Raw Data, Clinic Data, Non-Clinical Data, data from studies HL Data. No unlawful direct alteration of items is permitted according to Bioinfoclin R, W. It restricts the amount of harm that a Trojan horse within the system may cause.

Furthermore, to a certain extent, confidentiality and integrity policies can be used to combat the backdoor danger. This risk might let an unauthorized user access the system. The implementation of safeguards by

confidentiality and integrity policies will still to some extent limit access and its dissemination. Unauthorized users might not be able to view sensitive data, such as clinical or research data, under that scenario. These policies can be used to counter threats relating to authorisation. The authorisation function activates if the subject joins the system after being authenticated. Access objects are used to specify subject rights. Unauthorized actors cannot access private data due to access policies (related to confidentiality). The integrity policy will similarly prevent unauthorized parties from changing sensitive data. These regulations can be quite helpful in limiting the migration of malware that compromises the system and moves within (some malware moves laterally, some top-down, and some bottom-up). These access control mechanisms alone cannot protect against all dangers. There will also be a need for technical solutions to deal with these complex attacks. These access control measures are unable to stop ransomware that encrypts the data on the system. Patches must be installed, and security updates must be made available, for this. Additional solutions, such as EDR, HIDS, and HIPS, may be more important.

These regulations can't deal with threats brought on by a shoddy cryptography suite. Similarly, these regulations are ineffective in addressing dangers related to a lack of encryption. Strong cryptographic solutions must be implemented in order to combat these types of attacks and prevent unauthorized individuals from viewing or altering private data. Attacks that use social engineering are those whose mitigation calls for technological fixes and employee attentiveness. Access control regulations can be used to counteract these threats. Threats posed by" Man-in-the-Middle" cannot be reduced with these policies. Technical solutions are also needed to address this. To counter this threat, a secure, authenticated, and encrypted communication route is needed. One of the most recent incidents took place at Uber Inc [12]. wherein the adversary pretended to be a business IT specialist and persuaded an employee to divulge their login information. These access control measures are unable to counter threats to physical security. To deal with physical threats, appropriate protocols, solutions, and methods must be in place. Information system hardening regulations must be strictly followed to protect against threats related to poor setup. Following the adoption of hardening guidelines, it is necessary to conduct appropriate testing and maintenance in order to keep track of the controls that are implemented in accordance with hardening standards. Threats connected to the cloud must be addressed since this system uses AWS to handle data in the cloud. In principle, the client and AWS must come to an agreement outlining the necessary security criteria. The right processes must be in place with various partners, including Cartagenia, to enforce correct responsibility. These procedures should include NDAs (Non-Disclosure Agreements), rights to audit, security terms, business continuity clauses, etc.

10. Recommended Security Mitigation Aspects

10.1 Mitigation against Physical Threats

These protections will be of great help in dealing with physical threats. To secure their boundaries, The Center has put in place a few physical safeguards. It ought to be a component of organized procedures, in my opinion. To restrict physical access to its electronic information systems and the building where they are located, physical security rules and procedures should be tightly enforced. This will guarantee that only access that has been lawfully approved is permitted. This procedure entails evaluating current physical security weaknesses, identifying and putting into practice corrective actions, developing and carrying out a facility security strategy, etc. The "clean desk and clear screen" guideline ought to be followed strictly. All workstations that access ePHI must have physical security measures in place by the Center to limit access to authorized users. These measures must include card access, video surveillance, screen barriers, lock doors, security guards, and more. Device and Media Controls are an additional area that requires specific attention. While carrying out tasks related to device and media control, security controls should be kept in place. It comprises PHI disposal procedures, electronic media reuse, hardware and media accountability, and backup and storage procedures. Inadequate execution of these tasks increases the likelihood of data leakage, which might have serious repercussions.

10.2 Mitigation against Administrative Threats

It is necessary to designate security authorities at The Center who will be in charge of maintaining and carrying out policies and procedures. For all users and workers, security awareness and training programs should be developed and successfully executed. It will be a huge help in preventing social engineering assaults. A proper event management approach and procedures that must be strictly followed in HC are required to lessen the effect of threats. This will significantly lessen the amount of data loss and assist in some manner with data protection. For The Center which aids in reacting to emergencies and other occurrences like fire, vandalism,

system failure, and natural disasters that harm systems that include electronic protected health information, a business continuity and disaster recovery strategy must be in place. A business associate has been given permission by the Center in this instance to make, receive, keep, or transmit electronic protected health information. Therefore, the Center should have an acceptable guarantee on information security from a commercial partner.
They must determine all relevant information systems that store EPHI in order to comply with HIPAA regulations (Electronic Protected Health information). These information systems require regular inventory and updating. A risk assessment must be done before a risk management program is put into place. This will guarantee the foundation of HC's security posture. Periodic reviews of the policies and practices that HC developed and put into place are required. Based on the HC setup, these policies and procedures ought to cover all relevant security components.

10.3 Mitigation against Technical Threats
The center should adopt a NAC solution to greatly boost the robustness of controls in order to strengthen access control. If multi-factor authentication has no negative effects on company operations, it should be adopted. The Center should put into place a robust cryptographic system that uses PKI, integrity algorithms like SHA-256, and encryption techniques like AES 256. It ought to have been used for data in use, transmission, and at rest.

11 Final Remarks and Conclusion
The Center, a bioinformatics firm, is an expert in molecular pathology, clinical genetic labs, labs, and research. The Center must adhere to HITECH and HIPAA regulations since it handles PHI (Protected Health Information) and ePHI (Electronic Protected Health Information). The firm has adopted a few procedures in accordance with its data protection policy. For confidentiality, integrity, and properly enforced access control measures, DAC and MAC have also been taken into consideration. It does not, however, address every hazard that is pertinent to The Center. Additional controls must be implemented in order to counteract all dangers. The section above talks about these controls. The topic of necessary administrative, technological, and physical measures that must be included to strengthen The Center's security posture and comply with HIPAA rules is explored. By putting these extra controls into action, our organization will achieve the intended result and be better equipped to deal with diverse risks.

References
[1] Servies, A. W. "Architecting of HIPAA Security and Compliance on Amazon Web Services." (2018).
[2] Cartagenia Data Security & Confidentiality Policy V06: BCO(*), SVV, HVE, GJA, LEW (2014)
[3] Robinson, Glen, Ianni Vamvadelis, and Attila Narin. "Using Amazon web services for disaster recovery." Amazon web services 22 (2014).
[4] Hospital Center Policies: HC-C04101
[5] Scholl, M., et al. "An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule (NIST Special Publication 800-66, rev. 1). Gaithersburg, MD: Computer Security Division." Information Technology Laboratory, National Institute of Standards and Technology. Retrieved from http://csrc.nist. gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1. pdf (2008).
[6] Johnson, Stephen B., et al. "Using global unique identifiers to link autism collections." Journal of the American Medical Informatics Association 17.6 (2010): 689-695.
[7] Alder, Steve. "What is Considered Protected Health Information Under HIPAA." (2018).
[8] Bell, D. Elliott, and Leonard J. La Padula. Secure computer system: Unified exposition and multics interpretation. MITRE CORP BEDFORD MA, 1976.
[9] Brewer, David FC, and Michael J. Nash. "The Chinese Wall Security Policy." IEEE symposium on security and privacy. Vol. 1989. 1989.
[10] Sandhu, Ravi, David Ferraiolo, and Richard Kuhn. "The NIST model for role-based access control: towards a unified standard." ACM workshop on Role-based access control. Vol. 10. No. 344287.344301. 2000.
[11] Diver, Sorcha. "Information security policy-a development guide for large and small companies." Sans Institute (2007): 1-37.
[12] Rasalam, James, and Raymond J. Elson. "Cybersecurity And Management's Ethical Responsibilities: The Case Of Equifax And Uber." Global Journal of Business Pedagogy Volume 3.3 (2019).