Final Project Report

Daniel Cordeiro Marques

Jennifer Miller

Shrinivas Rathor

University of San Diego

CSOL-510-01-SP22 - Applied Cryptography

Dr. Michelle Moore

April 18, 2022

Executive Summary

Overview

Placebo Inc. is a health insurance organization, which means that sensitive data is handled by the company. The sensitive personal health information (PHI) needs to be securely accessed by customers, providers, and employees and securely transmitted to and from workstations, web servers, databases, and backups. There are legal requirements that also need to be met in order to protect this data. As a United States based company, compliance needs to be met for HIPAA, COPPA, and CCPA else there could be significant fines. Additionally, there are risks of malicious actors who want to gain access to this data, typically for financial gain. These threats can come from inside the company or externally.

Solution

Protecting PHI and electronic PHI (ePHI), which is essential to Placebo's business, requires the use of cryptography. Cryptography protects data by making it unreadable to unauthorized users. This report breaks down the recommended cryptography strategy for Placebo, which includes the required legal specifications and corporate controls and policies. The technical requirements, such as key length and specific cryptographic algorithms, needed to secure the ePHI encompasses both data at rest and data in transit are also specified.

Table of Contents

Security Goals

As a health insurance provider, safeguarding the customer's electronic personal health information (ePHI) is paramount for a successful security strategy. Placebo should strive to protect the confidentiality, integrity, and availability of ePHI against relevant threats (*Summary of the HIPAA Security Rule*, 2013), leveraging efficient security controls. It is also vital that such controls comply with applicable laws, regulations, and standards to minimize the risk of non-compliance and associated reputational and financial damages.

Laws, Regulations, and Standards

In addition to the federal and local privacy and consumer protection regulations regarding personally identifiable information (PII), such as the California Consumer Privacy Act (CCPA) and the Children's Online Privacy Protection Act (COPPA), health insurance companies must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Notably, the HIPAA Security Rule "establishes national standards to protect individuals' electronic personal health information" (*The Security Rule*, 2020), particularly the implementation of controls that safeguard information against unauthorized access and modification. Cryptography plays a central role in deploying such controls and supporting technologies that efficiently protect the integrity and confidentiality of ePHI.

HIPAA Requirements

HIPAA requires encryption if it is deemed a reasonable control to safeguard ePHI after a risk assessment (*Is the Use of Encryption Mandatory in the Security Rule?*, 2013). Encryption impacts two of its standards, "Access Control" and "Transmission Security" (*HIPAA Security Series #4 - Technical Safeguards*, 2007). This report approaches HIPAA's requirements from two perspectives:

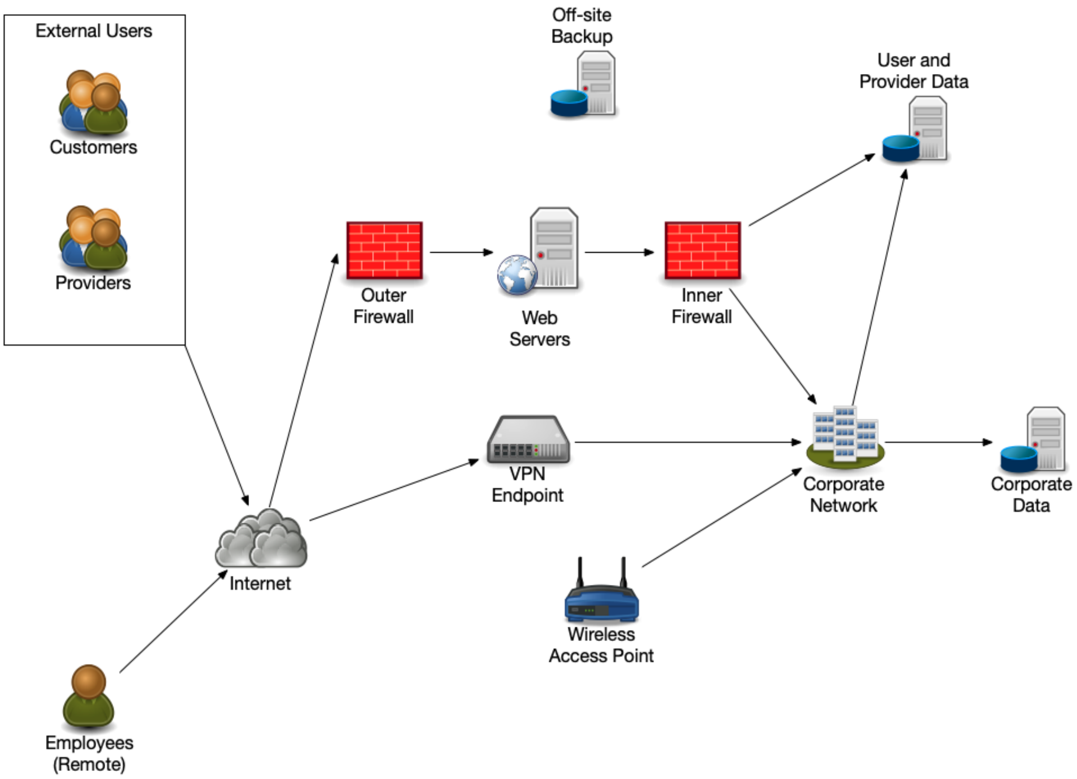
- **Data at rest -** Covers ePHI stored in digital media, servers, workstations, backups, or devices, such as customer data stored in a database for application consumption. The encryption strategy should provide recommendations that safeguard data stored in Placebo's systems.
- **Data in transit -** Relates to ePHI flowing in the network, including communications between users and web servers, VPN connections, and e-mail. The encryption strategy should cover controls that limit a threat's ability to access data if they intercept communications.

Network Diagram And Components

Figure 1 illustrates a high-level diagram of Placebo Inc.'s network.

Figure 1.

High-level network diagram.



Cybersecurity Threats and Risks

Cybersecurity Threats

The main objective of threats targeting health insurance providers is obtaining access to customers' ePHI for financial gain. In that context, the following threats stand out:

Ransomware and cybercrime groups. Ransomware groups target users and the corporate network through a variety of attack vectors, attempting to gain financially from the access obtained.

Internal (insider) threats. Disgruntled employees or compromised users, particularly employees and providers, may leverage their access to steal ePHI for financial gain.

Table 1 outlines the threats impacting each network component.

Table 1.

Threats and network components

Threats	Affected Components
Ransomware and cybercrime groups	● Web servers ● Corporate network ● External users ● Employees ● User and provider data ● Corporate data ● VPN endpoint ● Off-site backup ● Firewalls
Internal (insider) threats	● Web servers ● Corporate network ● External users ● Employees ● User and provider data ● Corporate data

Cybersecurity Risks

If a threat actor successfully exploits vulnerabilities in Placebo's environment, they may compromise customer's sensitive medical and personal information. As such, the organization may be exposed to the follow risks:

Communication interception. Remote employees and providers may connect to Placebo's systems from an untrusted network, such as a coffee shop. This may expose users to attackers attempting to intercept traffic between the client and the servers.

Threat actors may compromise user credentials. *2021 Data Breach Investigations Report* (2021) indicates an increased number of leaked usernames and passwords online. If a threat actor compromises valid credentials, they may impersonate the user and gain access to sensitive information.

Ransomware groups may compromise the internal network. Ransomware groups may successfully compromise the internal network through a variety of attack vectors and gain unrestricted access to systems storing ePHI.

Non-compliance with regulations resulting in financial loss. If a data breach occurs, Placebo may face fines of up to $250,000 (Alder, 2022).

Recommended Cryptography Strategy

When handling PII and PHI it is important to ensure that the data is only accessed by authorized parties, which is why it is important that the data is encrypted.

Scope and Assumptions

Placebo is a United States based company that does business within the United States. The company only has one physical office, which has an on-premise infrastructure and the rest of the employees are remote. This office has two floors, where there is one wireless access point (WAP) and all other access is through ports at the desks that can connect to the corporate LAN.

Controls are "the means of managing risk, including policies, procedures, guidelines, practices, or organizational structures" (*Control*). Placebo's physical, administrative, and technical controls that help protect the data and systems are shown in Tables 2 to 4.

Table 2.

Physical Controls.

Control	Component	Purpose
Exterior Lights and Security Cameras	Employees Visiting providers Servers & firewalls Off-site backup	Deter bad actors and have video surveillance to detect suspicious and malicious activity, which can also be used as evidence in case of an incident.
Badge System	Employees Visiting providers Servers & firewalls Off-site backup	Controls access to the building and role-based access to specific areas in the building (MDF & IDF, which have a default lock in case of emergency).
Security Guard	Employees Visiting providers Servers & firewalls Off-site backup	24 hour security guard to patrol and monitor guests and employees entering the building.

Table 3.

Administrative Controls.

Control		Purpose
Security Awareness Training	Employees	Informs employees of best practices and how to handle PHI data.
Single Sign On (SSO)	Employees Web Servers Corporate Network Inner Firewall Outer Firewall	Limits reuse of passwords and restricts use of local accounts.

Password Policy	Employees Web Servers	Best Practices for setting passwords.
Session Timeouts	Employees Web Servers Corporate Network	Ensures re-authentication is needed to continue to access systems. Privileged accounts have shorter sessions.
Multi Factor Authentication (MFA)	Employees Web Servers Corporate Network	Add an additional layer of authentication to verify a user's identity when signing into a system.
Patch Management & Vulnerability Scanning	Web Servers Corporate Network Inner Firewall Outer Firewall	Discover and resolve vulnerabilities on a regular basis.
Key Management System	Web Servers Corporate Network Inner Firewall Outer Firewall	Shared and secret keys must be stored in the corporate password manager, where they are encrypted and access is controlled. Keys are not to be shared in plain text, even within corporate communication systems.
Full Disk Encryption and Remote Wipe Capabilities	Employees Off-site Backup	All workstations and removable media are required to have full disk encryption before being deployed and where possible to have remote wipe capabilities in order to protect the data in case of physical theft.

Table 4.

Technical Controls.

Control		Purpose
Endpoint Detection and Response (EDR)	Employees	To help detect and mitigate threats such as malware or suspicious activity.
Network Access Control (NAC)	Corporate Network Inner Firewall Outer Firewall VPN	Only authorized and up to date computers can access the network. Only company owned machines are authorized to access the internal network, any unknown machine will not have access unless given permission to access the guest network. Also helps protect from malicious outsiders from accessing internal networks even if they are able to access a physical port in the office.

Intrusion Prevention System (IPS)	Corporate Network Inner Firewall Outer Firewall VPN	Monitors and scans the network traffic to detect and prevent suspicious and harmful traffic based on a set of rules.
Security Information and Event Management (SIEM)	Web Servers Corporate Network Inner Firewall Outer Firewall	Keeps the logs of alerts and provides audit data.

Security Policies Enforced

Security policies are a backbone of any organization and lay out the minimum baseline requirements that the organization must adhere to. Table 5 shows the policies that must be enforced.

Table 5.

Enforced Policies.

Policy	Purpose
Information Security	Protecting and preserving the confidentiality, integrity, and availability of Placebo's information assets and information systems.
Incident Response Plan	Provide a well-defined, organized approach for handling any potential threat to computers, data, and must identify and describe the roles and responsibilities of the Security Incident Response Team.
Vulnerability and Patch Management	Patch Management sets the requirements, schedule, and SLO's which apply to the distribution and application of patches. Vulnerability management policy is designed to remediate vulnerabilities and reduce inherent backlog, the purpose is defined as determining areas of weakness within the context of a centralized vulnerability management program.
Network Security	Protects the integrity of Placebo's network, to mitigate the risks and losses associated with security threats to computing resources and to ensure reliable network access and performance.
Password	Set well-defined requirements for passwords to access corporate systems (i.e. 10 character minimum, complex passwords, cannot use previous 8 passwords).

Data Classification	Designed to address risks to current and future data through the proper classification of all Placebo information, so it can be processed in a manner commensurate with its sensitivity.
Disaster Recovery and Business Continuity	Provides guidance on what is needed to keep the business running in the case of major outages and natural disasters. Provides details on backups and acceptable downtime periods.
Acceptable Use	Provide Placebo's workforce with guidance regarding the responsible, acceptable, unacceptable use of IT assets that are available to them for performing their job duties.
Physical Security	Provide guidance for safeguarding physical assets at company owned property.
Data Retention	Outlines how long different types of data need to be kept and how to dispose of data when no longer needed.

Controls To Safeguard Data At Rest

The controls outlined on Table 6 safeguard "data that is stored in the databases and is not moving through networks" (*Data At Rest Encryption*, 2021). To implement these recommendations, Placebo must only use industry standard tools that have been extensively tested.

Table 6.

Data at Rest Encryption Controls.

Control	Components	Requirements
Storage media (such as solid state disks) of Devices handling ePHI - including servers, desktops, laptops, and mobile devices - must be encrypted.	Employees External users Web servers Corporate data Customer data Offsite backup	● Disk encryption should use AES with a key at least 128-bit long (AES-128) for encryption and decryption (Scarfone et al., 2007).
Removable media should be encrypted.	Employees External users	● Removable media should use AES with a key at least 128-bit long (AES-128) for encryption and decryption (Scarfone et al., 2007).
Offsite backups must be	Offsite backup	● Backups should use AES with a key

stirred and encrypted.		at least 128-bit long (AES-128) for encryption and decryption (Scarfone et al., 2007).
The integrity of backups must be verified once a month against their hashes.	Offsite backup	● Hashes generated must be SHA-2 (*NIST Policy on Hash Functions*, 2015).

Controls To Safeguard Data In Transit

The controls outlined on Table 7 safeguard data transmitted between two systems. Similar to the data at rest controls, Placebo must only use industry standard tools that have been extensively tested.

Table 7.

Data In Transit Encryption Controls.

Control	Components	Requirements
Users must use VPN to access the corporate network remotely.	VPN endpoints Employees Providers	Following the recommendations established in NIST SP 800-77 (Barker et al., 2020), the following parameters must be enforced: **IKEv2** ● Encryption: AES-GCM or AES-CCM with a key at least 128-bit long ● Integrity: At least HMAC-SHA256 ● Diffie-Helman group: DH 14 to DH 21 ● Peer Authentication: RSA (3072-bit or larger key)or ECDSA with at 128-bit key. **IPSec-v3** ● Mode: Tunnel Mode, Transport Mode ● Protocol: ESP, IPComp ● Encryption: AES-GCM or AES- ● CCM with a key at least 128-bit long ● Integrity: HMAC-SHA256 ● Perfect Forward Secrecy (PFS): DH 14 to DH 21 (same or stronger than

		IKE)
Connectivity between clients and servers (for instance, HTTP, remote management interfaces) should be encrypted.	Employees External Users Web Servers Corporate Network Inner Firewall Outer Firewall	Communications should follow the specifications defined in the NIST SP 800-52 (McKay & Cooper, 2019) as follows: ● Connections should use at least Transport Layer Security (TLS) version 1.2. ● Servers should use valid certificates for authentication. ● Clients and Servers should only support cipher suites described in NIST SP 800-52 (McKay & Cooper, 2019). ● Clients and servers should support Perfect Forward Secrecy.
Electronic e-mail messages carrying ePHI should be encrypted.	Employees External Users	● Employees must encrypt their email using valid certificates and at least AES-128. ● External users must encrypt their email using PGP and at least AES-128. ● For transport encryption, email clients should follow the same recommendations as the connectivity between clients.

Conclusion

The cryptographic controls and requirements outlined in this paper will help Placebo protect the ePHI that flows through their systems. These recommendations will ensure that Placebo will be compliant with required US laws and prevent fines. Additionally, the customers may retain their trust in the company knowing the company is doing what they can to keep their sensitive information safe.

Glossary

A

Advanced Encryption Standard (AES) - “The AES algorithm is a symmetric block cipher that can encrypt and decrypt information” (nist.gov)

C

California Consumer Privacy Act (CCPA) - “CCPA gives consumers more control over the personal information that businesses collect about them” (oag.ca.gov)

Children’s Online Privacy Protection Act (COPPA) - The Children’s Online Privacy Protection Act (COPPA) “requires that websites, apps, and online services notify parents and get their express consent before collecting, using, or disclosing personal information from kids under 13” (Fair, 2022).

E

Endpoint Detection and Response (EDR) - “endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware” (*What Is Endpoint Detection & Response? | EDR Security Definition*, 2021).

ePHI - Electronic Protected Health Information

H

Health Insurance Portability and Accountability Act (HIPAA) - Federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge. (cdc.gov)

I

Identity and Access Management (IAM) - IAM is designed to ensure that access to information systems is provided to the authorized individuals.

Intermediate Distribution Frame (IDF) - "is a free-standing or wall-mounted rack for managing and interconnecting the telecommunications cable between end user devices and a main distribution frame (MDF)" (Hill, 2011).

Intrusion Prevention System (IPS) - IPS is a tool that scans the network for any threats or malicious activity and takes preventive measures.

L

Local Area Network (LAN) - "a collection of devices connected together in one physical location, such as a building, office, or home" (*What Is a LAN?*, n.d.).

Least Privileges - Providing minimum privilege to perform the assigned job duties.

N

Network Access Control (NAC) - "solutions support network visibility and access management through policy enforcement on devices and users of corporate networks" (*What Is Network Access Control (NAC)?*, n.d.).

National Institute for Standards and Technology (NIST) - "promote[s] U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life" (*About NIST*, n.d.).

M

Main Distribution Frame (MDF) - "the primary hub or demarcation point that interconnects private or public IT and telecommunication lines coming into a building to an internal network via any number of intermediate distribution frames (IDFs)" (*Main Distribution Frame (MDF)*, n.d.).

Multi-factor Authentication (MFA) - MFA is aimed to provide a multi-layer authentication to protect information systems by verifying the user identity.

P

Patch Management - “systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions” (*Patch Management).*

Penetration Testing - Authorized cyber attack on computer systems to understand the system security and any vulnerabilities.

Privileged Accounts - Having more permissions within a system than a normal user account. The account has elevated privileges, such as an administrator/admin permissions.

Protected Health Information (PHI) - PHI is a specific subset of PII that is related to individuals’ health data.

Personally Identifiable Information (PII) - Any data that can identify an individual.

S

Secure Hash Algorithm (SHA) - A type of cryptographic hash function

Security Information and Event Management (SIEM) - Collects a“broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities” (*Security Information and Event Management (SIEM)*).

Single Sign On (SSO) - SSo allows users to login to multiple applications with a single ID.

T

Transport Layer Security (TLS) - Security protocol used to protect data by encrypting the communication over the internet.

V

Virtual Private Network (VPN) - “Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line” (*Virtual Private Network (VPN)*, n.d.).

Vulnerability Scanning - Scanning information systems and networks for any weakness.

W

Wireless Access Point (WAP) - “A device that allows wireless devices to connect to a wired network using wi-fi, or related standards” (*Wireless Access Point (WAP)*, n.d.).

References

About NIST. (n.d.). NIST. Retrieved April 18, 2022, from https://www.nist.gov/about-nist

Advanced Encryption Standard - Glossary | CSRC. (n.d.). NIST Computer Security Resource Center. Retrieved April 18, 2022, from https://csrc.nist.gov/glossary/term/advanced_encryption_standard

Alder, S. (2022, January 3). *What Happens if You Break HIPAA Rules?* HIPAA Journal. Retrieved April 18, 2022, from https://www.hipaajournal.com/what-happens-if-you-break-hipaa-rules/

Barker, E., Dang, Q., Frankel, S., Scarfone, K., & Wouters, P. (2020). *Guide to IPsec VPNs* (SP 800-77 Rev. 1 ed.). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-77r1

California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General. (n.d.). California Department of Justice. Retrieved April 18, 2022, from https://oag.ca.gov/privacy/ccpa

Control. (n.d.). NIST Computer Security Resource Center. Retrieved April 18, 2022, from https://csrc.nist.gov/glossary/term/control

Data At Rest Encryption. (2021). IBM. https://www.ibm.com/docs/en/strategicsm/10.1.3?topic=security-data-rest-encryption

Fair, L. (2022, March 4). *When it comes to health data, comply with COPPA – no kidding*. Federal Trade Commission. https://www.ftc.gov/business-guidance/blog/2022/03/when-it-comes-health-data-comply-coppa-no-kidding

Health Insurance Portability and Accountability Act of 1996 (HIPAA). (2018, September 14). Centers for Disease Control and Prevention. Retrieved April 18, 2022, from https://www.cdc.gov/phlp/publications/topic/hipaa.html

Hill, D. (2011, March). *Intermediate Distribution Frame (IDF)*. TechTarget. Retrieved April 18, 2022, from https://www.techtarget.com/whatis/definition/intermediate-distribution-frame-IDF

HIPAA Security Series #4 - Technical Safeguards. (2007). HHS.gov. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

Is the use of encryption mandatory in the Security Rule? (2013). HHS.gov. https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html

Main Distribution Frame (MDF). (n.d.). Sunbird DCIM. Retrieved April 18, 2022, from https://www.sunbirddcim.com/glossary/main-distribution-frame-mdf

McKay, K., & Cooper, D. (2019). *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (SP 800-52 Rev. 2 ed.). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-52r2

NIST Policy on Hash Functions. (2015, August 5). National Institute of Standards and Technology. https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions

Patch Management. (n.d.). NIST Computer Security Resource Center. Retrieved April 18, 2022, from https://csrc.nist.gov/glossary/term/patch_management

Scarfone, K., Souppaya, M., & Sexton, M. (2007). *Guide to Storage Encryption Technologies for End User Devices* (SP 800-111 ed.). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-111

Security Information and Event Management (SIEM). (n.d.). Gartner. Retrieved April 18, 2022, from https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

The Security Rule. (2020, September 23). HHS.gov. https://www.hhs.gov/hipaa/for-professionals/security/index.html

Summary of the HIPAA Security Rule. (2013). HHS.gov. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

2021 Data Breach Investigations Report. (2021). Verizon. https://www.verizon.com/business/resources/reports/dbir/

Virtual Private Network (VPN). (n.d.). NIST Computer Security Resource Center. Retrieved April 18, 2022, from https://csrc.nist.gov/glossary/term/virtual_private_network

What is a LAN? (n.d.). Cisco. Retrieved April 18, 2022, from https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html

What is Endpoint Detection & Response? | EDR Security Definition. (2021, December 13). CrowdStrike. Retrieved April 18, 2022, from https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

What Is Network Access Control (NAC)? (n.d.). Cisco. Retrieved April 18, 2022, from https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

Wireless Access Point (WAP). (n.d.). NIST Computer Security Resource Center. Retrieved April 18, 2022, from https://csrc.nist.gov/glossary/term/wireless_access_point