# Final Project: Corporate Cryptographic Controls Recommendation

Group 7: Kevin McCaffrey, John McGovern, Daniel Mendoza

CSOL510 - Applied Cryptography

April 18th, 2022 - Spring 2022

Dr. Danny Barnes

## Executive Summary

Cryptographic controls and implementations of cryptographic algorithms are critical to the security of Placebo, Inc.'s (PI) data. PI is responsible to the patients, providers, and employees who entrust it with their data. Furthermore, PI has obligations under HIPAA, HHS directives, and additional relevant NIST and other guidelines. Failure to meet regulatory and legal requirements can result in significant fines to the organization per individual PHI recorded stored. To maintain the confidentiality and integrity of the data PI is entrusted with, cryptography is used to protect the data wherever it is stored and while it is being transmitted. Any PI system that accesses, transmits, or stores PHI comes under these controls and must use a variety of cryptographic controls. This includes desktops, laptops, mobile devices, medical devices, servers, and even cloud and SaaS offerings. Whenever available, the most secure cryptographic offering or offerings must be employed by PI and its vendors. A failure to use strong cryptographic standards can be cause for vendor dismissal from a bid process or removal of a technology from the environment. Finally, secure sign sign-on authentication is used to provide cryptographic assurances as to the employee or provider's identity. While some of these controls make systems implementation less convenient, they are critical in upholding the confidentiality and integrity of the data entrusted to PI. A focus on modern cryptographic controls pays dividends in meeting the organization's responsibilities to regulatory bodies and, most importantly, the patients and providers served by the organization.

## Table of Contents

## Introduction

As a healthcare organization, Placebo, Inc. (PI) is the custodian of a mission-critical repository of public health information (PHI). Because of this reality, cybersecurity must take a leading role when it comes to business and information systems operations and policy. In particular, cryptography must be used extensively throughout the organization as a means of controlling and protecting the flow of information throughout the organization and acting as a series of controls to ensure that the information entrusted to the organization is protected. This report describes the goals of using encryption at PI, the regulatory environment PI operates within, the types of cryptographic controls that are required, and the specific cryptographic mechanisms that are necessary to secure the environment.

## Corporate Cybersecurity Goals

First, it is helpful to understand the goals and objectives the organization is working to achieve with cybersecurity in general and encryption specifically, as the two terms are often confused or used interchangeably. Generally speaking, the goal of cybersecurity is to protect the confidentiality, integrity, and availability (CIA cybersecurity triad) of the organization's data. In other words, the aim of the security practice is to ensure that only authorized individuals and systems can see and change the data and that the data remains accessible to the correct entities at all times. Employees and authorized contractors should be the only personnel who are able to obtain and modify patent data. Providers must only be able to generate and access relevant information to achieve patient care. Encryption is a primary tool individuals and organizations use to accomplish these objectives. Without encryption, it would be near impossible to ensure data is sent in a confidential manner and without modification. Similarly, it would be difficult to

guarantee the safety of stored data from threats such as stolen or lost devices. These threats are discussed in more detail below.

It is helpful then to address Placebo, Inc's specific interest in strong encryption. The security of the extremely valuable data that patients, providers, and employees generate and entrust PI with is of key and critical importance, and as such, the organization must use tools such as encryption to protect it. Imagine a motivated cyber adversary sitting outside of the main healthcare network attempting to intercept important and valuable patient data as it is sent to another employee. Further, imagine that a laptop is lost or stolen and a file of patient records is recovered from the computer system by a malicious 3rd party. These scenarios are not uncommon and demand the attention of the PI organization (Davis, 2018). The organization is ethically obligated to protect PHI from these and many other attacks. In addition, it is legally obligated to implement security controls to protect this data in a responsible manner. The applicable laws and regulations are discussed in the next section.

## Laws & Regulations

### Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that created national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge (CDC, 2018). HIPAA defines sensitive data as "protected health information" and subjects it to a subset of rules (Privacy Rules). The Privacy Rule strikes an important balance between the effective use and privacy of data. Placebo Inc., as a healthcare organization, falls under HIPAA's Privacy Rules and, therefore, must consider the following compliance mandates:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information (CDC, 2018)
- Detect and safeguard against anticipated threats to the security of the information (CDC, 2018)
- Protect against anticipated impermissible uses or disclosures (CDC, 2018)
- Certify compliance by the workforce (CDC, 2018)

**Cybersecurity Act of 2015**

In the Cybersecurity Act of 2015, Congress established the Health Care Industry Cybersecurity (HCIC) Task Force to address the challenges the healthcare industry faces when securing and protecting itself against cybersecurity incidents (HCIC, 2017). Cases of identity theft, ransomware, and targeted nation-state hacking prove that health care data is vulnerable. Cybersecurity attacks also disrupt patient care and vital services to people in need. As part of its remit, the Task Force identified six high-level imperatives by which organizations such as Placebo, Inc. can identify threats, harden defenses, and proactively mitigate risks. The six HCIC imperatives are:

1. Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity (HCIC, 2017)
2. Increase the security and resilience of medical devices and health IT (HCIC, 2017)
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities (HCIC, 2017)
4. Increase health care industry readiness through improved cybersecurity awareness and education (HCIC, 2017)

5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure (HCIC, 2017)
6. Improve information sharing of industry threats, risks, and mitigations (HCIC, 2017)

**HITECH Amendment of 2021**

The HITECH Act was amended in 2021 to require organizations to take into consideration "recognized security practices" for resolving potential violations of the HIPAA Security Rule. The HITECH Act does not require organizations to implement these practices but does require that recognized security practices be consistent and in line with industry norms (Hennessy, 2022). As such, Placebo, Inc. should be aware of and periodically review:

- The standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the NIST Act (Hennessy, 2022);
- The approaches highlighted under section 405(d) of the Cybersecurity Act of 2015;
- Other programs and processes that address cybersecurity and that are developed, recognized, or recommended by statutory authorities (Hennessy, 2022).

**NIST Special Publication 800-175B Revision 1**

NIST SP 800-175B Rev. 1 (Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms) provides guidance to the Federal Government for using cryptography and NIST's cryptographic standards to protect sensitive information during transmission and while in storage (Barker, 2020). While Placebo Inc. is not a federal government organization, the encryption standards referenced in this Special Publication represents the latest guidance from NIST and should act as a reference in building Placebo's encryption infrastructure.

### NIST Special Publication (SP) 800-66 Rev. 1

NIST SP 800-66 Rev. 1 is intended to aid organizations in implementing the HIPAA Security Rule. Although this SP was updated in 2021, revision 2 is not yet published. SP 800-66 is a useful tool for Placebo Inc. as it helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. The SP also directs readers to helpful information in other NIST publications on individual topics addressed by the HIPAA Security Rule and aids readers in understanding the security concepts discussed therein (Scholl, 2008).

### Additional Relevant Standards and Controls

- CIS Critical Security Controls
- COBIT 5
- ANSI/ISA 62443-4-1-2018
- ISO/IEC 27001:2013

## Threat Environment

It is critical that the organization and cybersecurity group understand and analyze the threat environment and attack surface in question. The attack surface is composed of the devices, systems, and applications that are available for an adversary to use in their attack. Even if a device is not directly exposed to the Internet or easily vulnerable, it forms part of the attack surface in that an attacker can potentially use it to move through the environment. The goal of using encryption is to make it more difficult for the cyber attacker by reducing or removing the attack surface. An industry-standard defense-in-depth approach is used to provide assurance in

that even if one layer of protection is compromised, the other layers will likely remain intact to protect PI data (Hale, 2018).

A primary area of concern is data loss related to the loss or theft of PI devices. These devices include the fleet of laptops issued to employees and providers as well as mobile devices such as smartphones and tablets. The reality of the modern computing area is that mobility is critical. As such, encryption for data stored on these devices (data at rest) and encryption for data being sent back to PI servers (data in transit) are required. The goal of both of these layers of encryption is that any given device could be lost or stolen, and the data resident on that device would remain intact. Furthermore, if that device connects to the Internet, administrators can trigger a remote wipe of its storage for further assurance.

Another area of concern is data transmitted outside of the corporate network in general. As PI controls the physical network at corporate and provider facilities, there is one layer of associated protection. However, when a device is located remotely or on a home network (more common due to pandemic era usage), the attack surface broadens. In this case, multiple layers of encryption should be used to secure communications. Typically applications implement one layer of encryption. In addition, the computer provides a second layer of encryption through the use of virtual private network (VPN) software. This dual-layer combination lowers the attack surface and likelihood hood of a man-in-the-middle (MITM) attack quite dramatically. Wireless networks should also be considered as an area an attacker might target as no physical connection is required. Therefore, wireless network connectivity should provide its own secure encryption with the second layer provided by the application layer.

As mentioned prior, attack surface reduction is an activity that heavily benefits from multiple layers of security. As such, it is important to consider the applications that actually

house and transmit corporate data. As much as the cybersecurity group attempts to provide a hardened shell around these apps on devices and servers, the application itself should resist attack. This is done through the application's use of its own encryption. A key example is the adoption of a secure messaging platform for the organization that provides its own encryption (Datskovsky, 2018). The goal is to make sure an attacker never gets close to being able to interact with the application, but breaches are inevitable. As such, each application must be built and audited to show that attack surface reduction has been considered.

Finally, it is important to note study threat actor methods and locality. An attacker may be across the ocean working to attack systems locally, or an attacker may deliberately or opportunistically attempt to seize devices locally or through a proxy. An attacker could even be a malicious or disgruntled insider who is attempting to steal data. The encryption used to support confidentiality and integrity concerns should similarly be used to thwart the efforts of a variety of attacker modalities and proximities.

## Corporate Security Policies & Controls

A variety of policies are used at Placebo, Inc. (PI), which supports the use of encryption and helps to ensure the PI is in compliance with a wide variety of applicable laws and regulations as described previously in this report. These policies are described at a high level below and more specifically in individual policy and technical control documents beyond this report's scope.

### Corporate Device Management

Devices such as laptops, desktops, medical devices, and servers that have access to, store, or transmit protected health information (PHI) must be owned by PI or leased under contract.

These devices must have installed corporate endpoint management and security software as appropriate based on the device and operating system. Devices without such software must not be able to access PHI or other protected PI resources.

**Mobile Device Management**

PI recognizes the utility and ubiquity of mobile devices such as smartphones and tablets in the workplace. These devices are often privately owned. However, constraints are in place to ensure that devices used to access PI data are secured and encrypted appropriately. For a mobile device to be used to access PI data, that device must be (1) capable of full disk encryption, (2) capable of using the PI approved secure messaging application (where messaging is required), (3) capable of being managed using corporate mobile device management (MDM). MDM software is used to enforce encryption and security policies and allow for the security team to remotely wipe a device if lost or stolen.

**Encryption for Data at Rest**

All systems that access, transmit, or store Placebo, Inc. (PI) protected information must use full disk encryption to protect the storage medium on which the data resides. Data may not be resident on non-encrypted media for any length of time. 3rd party systems used under contract, such as those provided by a Software as a Service (SaaS) provider, must use encrypted storage enforced under vendor contract with PI. Encryption of storage should use the best available NIST standard encryption available, as described further in the Cryptographic Mechanisms section below.

**Encryption for Data in Transit**

PHI sent over the PI corporate network, or a provider network under direct PI management must be encrypted at least once using the strongest available encryption mechanism as described below in the Cryptographic Mechanisms section. When data is transmitted from a source outside of the corporate network (including any wireless network), this information must be encrypted twice (two distinct layers of encryption). This may include encryption provided by a VPN solution, a Secure Access Service Edge (SASE), wireless network encryption such as EAP-TLS, or another equivalent solution. A common solution would be a TLS connection to an application server that is transmitted over an encrypted VPN tunnel or encrypted corporate wireless network. A personal wireless network or hotspot using shared secret encryption does not qualify as a layer of encryption.

**Application Layer Encryption**

Applications that access, store, or transmit PHI must provide encryption in transit (such as TLS encryption for applications using HTTPS). Whenever possible, these applications should also encrypt data at rest in application storage (such as in a database or cloud storage mechanism). All applications under this protected scope should leverage the robust access control mechanisms provided by the PI single sign-on (SSO solution). All new applications implemented by PI must use the corporate SSO solution, while legacy applications should use the solution wherever possible and be supported by the relevant vendors.

## Hardware-Level Encryption

Whenever possible, a system such as a laptop, desktop, mobile device, or service should utilize a Trusted Privacy Module (TPM) to authenticate core operating system level components and provide a secure and tamper-proof encryption key storage mechanism.

### Cryptographic Key Storage

Given the wide variety of applications for symmetric and asymmetric cryptographic keys, recommending a single storage solution is not possible. That said, the organizational policy is toward seeking out and implementing the most secure solution available and commercially feasible. This includes hardware security modules (HSMs) to generate and store private keys and key vaults (sometimes known as central key management systems (CKMSs)) to secure symmetric keys and key pairs as required. Solutions such as application delivery controllers (ADCs), which allow the administrator to securely store but not retrieve the private key, are preferred over alternatives. In cases where key retrieval is required (SSL inspection, for example), a secure key vault must be used that implements robust cryptographic access control and auditing.

### SSL Inspection

In some cases, PI requires that SSL traffic be decrypted and then encrypted for security or performance monitoring reasons. In this case, the most secure form of encryption available must be used for both the user-facing and backend. Downgrading should be done carefully and only once the traffic has reached a trusted corporate network. All inspected traffic must be encrypted before reaching the destination server.

### Industry Standards

"Roll your own," academic, hobbyist, or experimental encryption is not allowed to be used within the PI environment. Cryptographic standards used should be selected from the Cryptographic Mechanisms section below. Cryptographic algorithms used by the PI organization are based on NIST standards and are vetted by the National Security Agency (NSA) and other similar U.S. government authorities. Vendors who support FIPS 140.2 and similar standard encryption are preferred.

## Cryptographic Mechanisms

The cryptographic mechanisms and algorithms described below represent a view into the best practice guidance supplied by organizations such as the U.S. National Institute of Standards and Technology (NIST) in publications such as NIST SP800-175b and others. Therefore, they are recommended for use within the PI secure environment and prioritized whenever possible by devices, applications, and vendor-provided SaaS systems.

### Symmetric Cryptography

The Advanced Encryption Standard (AES) is the recommended symmetric encryption cipher mode and should be used whenever available. 128-bit keys are the minimum recommended, and stronger keys are preferred whenever possible (Barker, 2020). AES is used for a wide range of purposes such as encryption of data at rest, as part of transmitting data securely, and authentication of messages.

### Asymmetric Cryptography

The Rivest, Shamir, and Adelman (RSA) algorithm is the preferred solution for asymmetric cryptography. Asymmetric cryptography is often used as the initial mechanism to

exchange symmetric keys. RSA has been widely adopted by certificate authorities, in cryptographic tools such as OpenSSL, and in use within Public Key Infrastructure.

**Hash Function**

The SHA-2 family of hash functions should be used whenever possible as a means of file authentication, digital signatures, and for other related purposes. 256-bit hashes or longer are required.

**SSL/TLS Cryptography**

Secure Socket Layer and Transport Layer Security (SSL/TLS) represents a set of common and ubiquitous standards. These standards are known for Hypertext Transport Protocol Secure (HTTPS) encryption but are used in other applications and protocols such as the Simple Mail Transfer Protocol (SMTP) and various messaging applications. All SSL versions are now deprecated and should not be used in the PI environment. TLS 1.0 and 1.1 versions are largely considered insecure and should not be used. TLS versions 1.2 and 1.3 are supported and indeed required for use when TLS encryption is available and required. Perfect forward secrecy (PFS) should be enabled and used whenever possible and in cases where TLS traffic inspection is not required.

**Public Key Infrastructure (PKI)**

Finally, public key infrastructure (PKI) should be used along with 3rd party trusted root certificate authorities (CAs) to validate the legitimacy of a given certificate. Whenever a web property or application is end user facing, a valid 3rd party CA issued certificate must be used. The enterprise may deploy its own PKI internally for device authentication and secure management of systems. However, valid 3rd party certificates are always preferred whenever

appropriate. A user, provider, or employee must, as part of their access, need to or be told to bypass certificate validation or use insecure websites and should instead report any such instances as suspicious. The X.509 certificate format is preferred and used extensively. The RSA algorithm with SHA-256 hashes and with at least a  2048-bit key length is required.

### Virtual Private Network (VPN) Cryptography

Finally, virtual private network (VPN) connectivity must be used whenever a provider or employee is not connected to the corporate managed wired or wireless network (encryption required on wireless). This includes remote connections and home office work where access to PHI is required. Connections between PI sites should also use site-to-site VPN connectivity where a private network link is not possible. Both SSL and IPSEC-based VPNs are acceptable. Long random keys must be generated and used in shared key scenarios, and rotation is recommended as frequently as feasible for the given technology. VPN connections should use strong cryptographic standards, as mentioned above. VPN authentication is required and should use multiple factors integrated with the corporate single sign-on solution for a cryptographically delivered challenge.

## Conclusion

By implementing encryption throughout the organization at each system or service that is used to access, transmit, or store PHI data, Placebo, Inc is making a wise investment in both meeting its ethical obligations to its customers and meeting legal requirements placed on the organization. The strongest available industry-standard encryption should be used wherever available to meet legal and regulatory requirements to protect PHI. Data should be encrypted whenever it is in transit or at rest over a network or on a storage medium of some sort. Organizational policies enforcing such requirements help Placebo, Inc. to better serve its

employees, providers, and patients, leading to improved overall business outcomes for the organization.

## Glossary of Cybersecurity Terms

**Advanced Encryption Standard (AES)** - The primary U.S. government approved symmetric key encryption algorithm (block cyber). A high performance algorithm that can be used to encrypt large amounts of data for at rest or in transit use cases (NIST, n.d.).

**Application Delivery Controller (ADC)** - A device used (primarily in pairs) as a load balancer to scale and protect web and other types of applications. Often used as a termination point for SSL/TLS and to house the appropriate cryptographic certificates (F5, n.d.).

**Asymmetric Cryptography** - A cryptographic system that uses a public and private key pair to allow all public key holders to encrypt traffic that only a private key can be decrypted. The public key is assumed to be publicly available and requires no special protection (NIST, n.d.). Also known as public key encryption.

**Central Key Management System (CKMS)** - A system that performs key management tasks on behalf of another system in a highly secure manner (Thales, n.d.).

**Certificate Authority (CA)** - A central trusted entity that is responsible for issuing and cryptographically signing cryptographic certificates (NIST, n.d.). A trusted 3rd party root CAs certificate is included in browser trust stores as a means of implying trust to certificates signed by that authority.

**Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)** - Encryption protocol used by wireless networks that relies on TLS encryption with client and server certificates for authentication (Grubbs, n.d.).

**Encryption Algorithm** - A particular method of encrypting data as implemented in computer code.

**Encryption at Rest** - Encryption used to protect data that is resident on a storage medium (Lord, 2019).

**Encryption in Transit** - Encryption that is used to protect data as it is being transmitted over a network or moved between storage locations (Lord, 2019).

**Hardware Security Module (HSM)** - A physical device built to generate, store, and operate on cryptographic keys and resist the extraction of those keys through tampering and other nefarious means (NIST, n.d.)

**Hash Function** - A function or algorithm that takes as input an arbitrary length of bits and outputs a deterministic generated but completely random and irreversible signature (NIST, n.d.).

**Health Insurance Portability and Accountability Act (HIPAA)** - A 1996 act that created U.S. national standard to protect patient health information from unauthorized disclosure and use without the patient's knowledge and consent. This act was implemented through a variety of privacy rules which affect how this information is protected (CDC, 2018).

**Internet Protocol Security (IPsec)** - A network communication protocol that adds security by way of encryption to standard network layer IP traffic (NIST, n.d.).

**Man-in-the-Middle Attack (MITM)** - An attack in which the attacker inserts itself in between the center and receiver and pretends to be one or both (NIST, n.d.).

**National Institute of Standards and Technology (NIST)** - A United States government agency that is responsible for advancing standards in science and technology (NIST, 2009). NIST publishes many of the standards relevant to HIPAA regulation and corporate cybersecurity in general.

**Perfect Forward Secrecy (PFS)** - An property of cryptosystems by which keys are rotated at an interval, making the recovery of old data with a recent key extremely difficult (Greenberg, 2016).

**Protected Health Information (PHI)** - Any health data created, received, stored, or transmitted by an entity falling under HIPAA or in a business associate relationship with the HIPAA entity (HIPAA Journal, 2022).

**Public Key Infrastructure (PKI)** - A network of systems and applications that allow for the creation, distribution, authentication, and operating of public key (asymmetric) cryptography within an organization or the Internet. Used for identity verification through digital signatures. A common application is to distribute signed SSL/TLS certificates for use in encrypting web traffic (NIST, n.d.).

**Rivest, Shamir, and Adelman (RSA)** - An algorithm used for the creation and validation of public key-based digital signatures (NIST, n.d.).

**Secure Access Service Edge (SASE)** - A cryptography enabled framework that is used by an organization to connect their users and devices securely to a cloud-based “edge” network that can inspect and route traffic in a more secure manner as is appropriate based on the nature of the connection (Zscaler, n.d.).

**Secure Sockets Layer (SSL)** - An Internet security protocol that uses encryption to protect the web and other types of traffic. This standard has been superseded by TLS, but often these terms are still used interchangeably (i.e., SSL certificates) (Cloudflare, n.d.-a).

**Single Sign-On (SSO)** - A cryptographically enabled service that allows the end user to sign into a wide variety of services using one login experience and credential set. Rather than

implementing its own login system fully, an application can use a protocol such as the Security Assertion Markup Language SAML (2.0) to ask the SSO service to authenticate or deny authentication to a user and provide a response back to the application. SSO uses TLS encryption and certificates in a similar way to HTTPS (Lu, 2019).

**Symmetric Cryptography** - Symmetric cryptography is a ubiquitous form of cryptography that principally uses the same key to encrypt and decrypt the given data. Symmetric cryptography is significantly faster computationally and is often used to encrypt data in transit and at rest once an initial key exchange has occurred. AES is a standard algorithm for symmetric encryption (NIST, n.d.).

**Transport Layer Security (TLS)** - A widely adopted security protocol that is designed to cryptographically enable secure communication over the Internet for services such as secure websites and others. The successor to the SSL protocol (Cloudflare, n.d.-b).

**Trusted Platform Module (TPM)** - A hardware module built into computer systems that is designed to provide secure cryptographic operations to the operating system in a tamper-resistant manner. The goal of such a module is to ensure that malicious software is not able to perform certain cryptographic operations and retrieve sensitive data such as cryptographic keys (Microsoft, 2022).

**Virtual Private Network (VPN)** - An encrypted network link used to connect a remote device to a network such as a secure corporate network or to connect two networks together. Often implements TLS or IPSEC encryption to protect traffic in transit (NIST, n.d.).

## References

Barker, E. (2020, March). *SP 800–175B Rev. 1, Guide for Using Crypto Standards: Cryptographic Mechanisms*. Computer Security Resource Center. https://csrc.nist.gov/publications/detail/sp/800-175b/rev-1/final

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

Cloudflare. (n.d.-a). *What is SSL?* https://www.cloudflare.com/learning/ssl/what-is-ssl/

Cloudflare. (n.d.-b). *What is Transport Layer Security (TLS)?* https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

Datskovsky, Galina (2018, December 05). *Why Businesses Need Secure Messaging That Goes Beyond Encryption*, Techopedia, retrieved from https://www.techopedia.com/why-businesses-need-secure-messaging-that-goes-beyond-encryption/2/33678

Davis, J. (2018, January 12). *Data of 43,000 patients breached after theft of unencrypted laptop*. Healthcare IT News. https://www.healthcareitnews.com/news/data-43000-patients-breached-after-theft-unencrypted-laptop

F5. (n.d.). *F5 Glossary*. F5 Glossary. https://www.f5.com/services/resources/glossary/application-delivery-controller

Greenberg, A. (2016, November 28). *Hacker Lexicon: What Is Perfect Forward Secrecy?* Wired. https://www.wired.com/2016/11/what-is-perfect-forward-secrecy/

Grubbs, P. (n.d.). *What is EAP-TLS?* SecureW2. https://www.securew2.com/blog/what-is-eap-tls

Hale, Charles (2018, May 01). *Security in Depth*, ISACA Journal. https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/security-in-depth

Health Care Industry Cybersecurity Task Force (2017, June 02). *Report on Improving Cybersecurity in the Health Care Industry*. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Hennessy, Jennifer (2022, April 11). *HHS Requests Comments on HIPAA/HITECH Act: Recognized Security Practices & Methodologies to Compensate Harmed Individuals*, Foley and Lardner LLP. https://www.foley.com/en/insights/publications/2022/04/hhs-requests-comments-on-hipaa-hitech-act

HIPAA Journal. (2022, January 2). *What is Protected Health Information?* https://www.hipaajournal.com/what-is-protected-health-information/

Lord, N. (2019, July 15). *Data Protection: Data In transit vs. Data At Rest*. Digital Guardian. https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

Lu, D. (2021, February 19). *What Is Single Sign-On (SSO)?* Okta. https://www.okta.com/blog/2021/02/single-sign-on-sso/

Matthew Scholl, Kevin Stine, Joan Hash, Pauline Bowen, Arnold Johnson, Carla Dancy Smith, and Daniel I. Steinberg (October 2008). *NIST Special Publication 800-66 Revision 1; An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

Microsoft. (2022, March 24). *Trusted Platform Module Technology Overview*. Microsoft Docs. https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview

NIST. (n.d.). *Glossary*. Computer Security Resource Center. https://csrc.nist.gov/glossary/

NIST. (2009, July 10). *About*. https://www.nist.gov/about-nist

Thales. (n.d.). *What is a Centralized Key Management System?* https://cpl.thalesgroup.com/faq/key-secrets-management/what-centralized-key-management

Zscaler. (n.d.). *SASE: What is Secure Access Service Edge?* https://www.zscaler.com/resources/security-terms-glossary/what-is-sase