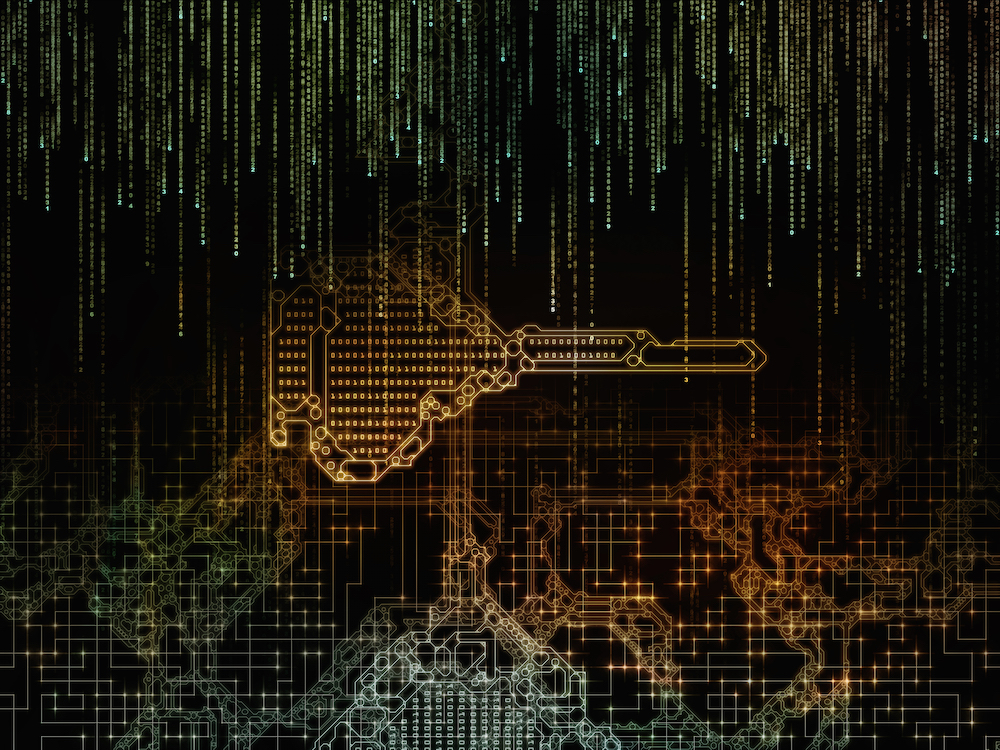
**CONFIDENTIALITY POLICY & CRYTOGRAPHY ARCHITECTURE**

**COMPANYX INSURANCE CO.**



**Presented by:** Ryan nye

university of san diego

**Disclaimer:** The chosen case scenario is for learning purposes only. The plan presented in the case scenario is fictitious and are not intended to be implemented without professional consultation. Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the U.S., State, local governments or University of San Diego, and the information and statements shall not be used for the purposes of advertising.

Contents

[1 CONFIDENTIALITY POLICY & CRYpTOGRAPHY ARCHITECTURE 1](#_Toc496565890)

[2.1 EXECUTIVE SUMMARY 4](#_Toc496565891)

[2.1.1 CRYTOGRAPHIC IMPLEMENTATION PER PROCESS EXECUTIVE SUMMARY 6](#_Toc496565892)

[2.1.2 UNDERSTANDING THE Healthcare Ecosystem 7](#_Toc496565893)

[3 LAWS, REGULATIONS, AND STANDARDS 8](#_Toc496565894)

[3.1 Payment Card Industry Data Security Standard (PCI DSS) 8](#_Toc496565895)

[3.2 Health Insurance Portability and Accountability Act (HIPAA) 10](#_Toc496565896)

[3.2.1 Protected Health Information (ePHI): 10](#_Toc496565897)

[3.2.2 HIPAA Violations 11](#_Toc496565898)

[4 CONFIDENTIALITY POLICY 12](#_Toc496565899)

[4.1 HASH & mac fUNCTIONS 13](#_Toc496565900)

[4.2 Problem: Key Exchange 13](#_Toc496565901)

[4.2.1 Solution: Kerberos Server 13](#_Toc496565902)

[4.2.2 Multiple Kerberos “Realms” 14](#_Toc496565903)

[4.2.3 HYBRID PKI SYSTEM 14](#_Toc496565904)

[4.2.4 MANAGEMENT OF KEYS AND CERTIFICATES 14](#_Toc496565905)

[4.3 RSA SETUP 15](#_Toc496565906)

[4.4 THREAT MITIGATION & SUPPORTING CONTROLS 15](#_Toc496565907)

[4.4.1 HEALTCHCARE THREAT SUMMARY 15](#_Toc496565908)

[4.4.2 MINNIMUM CONTROLS 15](#_Toc496565909)

[4.4.3 Added Cryptographic Mechanism Controls 16](#_Toc496565910)

[4.4.4 OPERATING SYSTEM Related CONTROLS 16](#_Toc496565911)

[4.4.5 Hardware & Software Considerations 16](#_Toc496565912)

[4.4.6 NO KNOWN THREATS TO SHA-256 17](#_Toc496565913)

[4.4.7 HMAC-SHA256 17](#_Toc496565914)

[4.4.8 destruction of stored or recorded media containing phi 17](#_Toc496565915)

[4.4.9 RSA Protocol Threats 17](#_Toc496565916)

[4.4.10 DH Protocol Threats 18](#_Toc496565917)

[4.4.11 CERTIFICATE THREATS 18](#_Toc496565918)

[5 CONCLUSION 19](#_Toc496565919)

[6 APPENDIX I: CRYPTOGRAPHIC diagram 20](#_Toc496565920)

[6.1 Components 21](#_Toc496565921)

[6.2 Interfaces 28](#_Toc496565922)

[7 APPENDIX II: Authentication BY LDAP, KERBEROS, OR CERTIFICATE 31](#_Toc496565923)

[8 APPENDIX III: kerberos simplified 32](#_Toc496565924)

[9 APPENDIX IV: CITRIX & HARDWARE (EXample: Aesec) IMPLEMENTATION 33](#_Toc496565925)

[10 APPENDIX V: EXAMPLE NETWORK to show when VPN/SECURITY is ACCESSED 34](#_Toc496565926)

[11 APPENDIX VI: WHAT DOES PHI INCLUDE? 35](#_Toc496565927)

[12 Appendix VII: Cost of Data Brach per Industry 36](#_Toc496565928)

[APPENDIX VIII: RISK DESCRIPTIONS for DEVICE 37](#_Toc496565929)

[13 APPENDIX IX: RISK DESCRIPTIONS for NETWORK 38](#_Toc496565930)

[14 Appendix X: Storage Encryption Technologies 39](#_Toc496565931)

[15 Appendix XI: PKI OVERVIEW 40](#_Toc496565932)

[16 APPENDIX XII: SAFE-BioPharma Certificate Excerpt 41](#_Toc496565933)

[17 APPENDIX XIII: Acronym Definition 42](#_Toc496565934)

[18 REFERENCES 43](#_Toc496565935)

## EXECUTIVE SUMMARY

This document presents a network diagram for CompanyX Health Insurance Company. The cryptographic techniques and programs outlined in this plan secure electronic protected health information (ePHI) for customers and payments to and from business partners. The ePHI stored and transmitted is regulated by the U.S. Health Insurance Portability and Accountability Act (HIPAA). The recommended cryptography standards for HIPAA are set by NIST (National Institute of Standards and Technology). Most encryption processes and programs set forth in this plan follow NIST standards are listed in [Section 4](#COnPolicy) titles “Confidentiality Policy”

**Policy**The cryptographic architecture first begins with *a written policy* to outline encryption strategies to protect consumer data. Second, this policy is endorsed by management to ensure policy has support from the highest levels. Third, the policy for consumer protections is communicated to the end-users, payors, providers, cloud services, and all other third parties.

**Cryptography Diagram: 4 User Types**The diagram accounts for the four types of users: customers (buyers of medical insurance), providers (medical organizations providing services to customers), workers on-site (corporate), and off-site (remote location). CompanyX Insurance workers are on workstations connected directly to the corporate (local area network) LAN, and remote workers connected to corporate LAN via a virtual private network (VPN). Corporate workstations are connected to servers behind an inner firewall, where a wireless access point (WAP) is used by guests only. See [Appendix I](#Diagram) for a full outline of components and interfaces associated with the architecture.

**Trust Framework**The project has determined which hosts using CompanyX applications, and the network the host is running on, are secure. The tiers of hosts are divided into customers, providers/partners, corporate workers on-site, and corporate workers off-site using VPN**.**The connections to CompanyX will be authenticated with the Kerberos server, LDAP, or PKI and is displayed graphically   
on [Appendix 2](#Authgraph).

| TRUST MODEL | | | |
| --- | --- | --- | --- |
| USER | TRUSTED HOST? | TRUSTED NETWORK? | AUTHENTICATION |
| Customers | NO | NO | **Kerberos Realm 1** – Records Access **2FA** – Message sent to email/phone to help secure host |
| Providers / Partners | YES | NO | **Kerberos Realm 2** – Database Access **PKI / Cert** – Communications / Payment / EDI to CompanyX Insurance |
| Corporate Workers on Site | YES | YES | **LDAP** – Database Access  **PKI / Cert** – Communications / Payment / EDI from Providers |
| Corporate Workers on VPN | YES | NO | **Kerberos** **Realm 3**– Database Access **PKI / Cert** – Access to Local network |

**LDAP**Lightweight Directory Access Protocol (LDAP) is an authentication protocol for accessing server resources over an internet or intranet network. The Active Directory (AD) is used to identify trusted local users on the network. But what if the user is trusted but on an insecure connection? For that, we use the Kerberos server for authentication and protection during the transmission of cryptographic keys (MIT, 2008).

**The New Kerberos Server System**   
See [Appendix 3](#KerbSimp) for an example on how the Kerberos works. Kerberos uses a ticket granting system to first identify its users before allowing access to a server with sensitive files (e.g. ePHI, Corporate data). Identifying employees is for Kerberos since it can link to the Active Directory (use components of the LDAP). Therefore, the issue is with the customers who will be hard to keep track of. We discuss our solution as a Kerberos / PKI hybrid using multiple realms to segregate user groups.

**Public Key Infrastructure (PKI)**   
A Public Key Infrastructure (PKI) can provide the appropriate mechanisms to effectively support authentication, authorization and confidentiality services such as communications between all the stakeholders, namely physicians, patients and e-health service providers (Kambourakis et al., 2005)**.** The PKI system allows a user/admin to recognize which public key belongs to whom, and provides limitations on how long a user is granted access to send or receive information. See [Appendix XI](#PKIOverview) for an overview on PKI.

**Certification authority (CA)**   
An entity that issues digital certificates to assure the organization is dealing with the authorized party. Example organizations include Symantec (Verisign), Comodo, and GoDaddy. This digital certificate from the CA confirms the ownership of a public key by the named entity on the certificate (originator of the message). An example of an entity would be the provider or the remote worker accessing the Healthcare network via a VPN. The format of these certificates is specified by the X.509 standard -accepted by HIPAA. The X.509 certificate provides the security administrator the flexibility for matching profiles to real life user roles (SANS, 2001). See [Appendix VII](#certexcerpt) for an example of an X.509 cert.

**Algorithms**Algorithm candidates that were considered for selection were AES, Serpent, and TwoFish. DES is proven insecure and was not eligible in the selection process. CompanyX will use only AES and TwoFish 256-bit keys. NIST recommends AES for HIPAA compliance. The key length of 256 guards against collision attacks such as birthday or meet-in-the-middle. Algorithms for each component and interface is listed on [Appendix 1](#Diagram).  
 **Block Cipher**The modes of these ciphers will use CBC with Random IV for storing ePHI. For efficiency on the LAN, we will be using CTR mode since it’s a low risk area. CTR does have its weaknesses, but is minimized when only operating on the trusted local network. Ciphers for each component and interface is listed on [Appendix 1](#Diagram). **Supporting Controls for Encryption Mechanisms**Supporting controls will be needed to ensure the cryptographic system is not compromised by known creative methods. For example, an attacker can measure the time to perform an AES operation to learn bits about the key, Therefore, careful plans will be made to conceal the timing information that will be discussed in another summary. Additionally, the keys of the encryption may be compromised by way of side-channel attacks, where computer artifacts relating to the key are analyzed. Minimum controls will need to be in place and tested which include: file permissions, passwords, two-factor authentication, and educating staff on spear phishing and vishing techniques. All access controls will be audited on a regular basis to ensure compliance to the new 2018 policy. Supporting controls are included on [Section 4.2](#ThreatMitControl) titled “Threat Mitigation and Supporting controls “.

**TPM**The TPM hardware will serve as the main supporting controls. The embedded hardware in the user device contains the private keys to connect to three main networks government by a Citrix client. See [Appendix IV](#AESCHARDWARD) for a graphical representation.

1. Local LAN
2. Provider Network
3. Web Applications

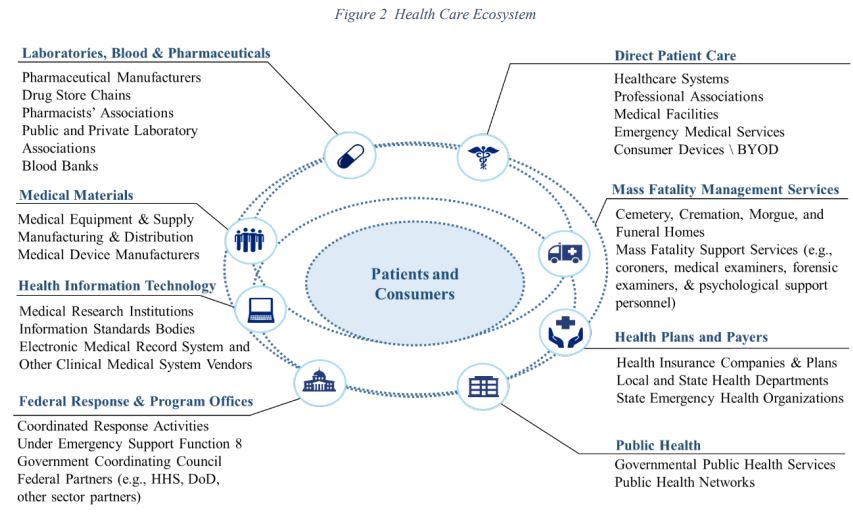
**Electronic Fund Transfer (EFT)**The two most protected channels for an insurance based organization will be securing plan payments from customers and sending bulk payments to providers. The team selected "TECS" telecommunications & e-commerce solutions GmbH as the mobile payment infrastructure. This move to a more secure payment system maintains CompanyX’s compliance with PCI Security Standards and increases our security stance.

SEE NEXT SECTION FOR TECHNICAL SUMMARY

### CRYTOGRAPHIC IMPLEMENTATION PER PROCESS EXECUTIVE SUMMARY

|  |  |  |  |
| --- | --- | --- | --- |
| **CRYPTOGRAPHIC IMPLEMENTATION SUMMARY** | | | |
| **User** | **Process** | **Crypto System(s)** | **Additional Controls** |
| **Customers** | User log-In to Account | **Data in Use:** Kerberos Authentication Realm 1Homomorphic Encryption (TBA) | **2FA** – Email code |
|  | Patient payments on CompanyX website | **Data in Transit** TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_\_SHA256 | **Application TECS** for secure EFT Payments |
|  | Mobile AP Login | (Encrypted App Development TBA) | TBA |
|  | Calls through AP | (Encrypted App Call Development TBA) | TBA |
| **Providers** | Provider log-in to account | **Data in Transit** SSH Connections to LAN (files) TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_\_SHA256 | **CISCO ACL Inner Firewall** -  IP Black/White lists |
|  | CompanyX payment to provider | **Data in Transit** Kerberos Authentication Realm 2 PKI/Digital Certificate Signing(PGP) SSH / VPN | FAX / Phone Call / Meetings between IT to Verify PKI Certs |
| **Local / Remote Corporate Workers** | **Accessing Corporate Data:**  Accounting Finance Sales Executive / Planning | **Data in Storage (Device):** BitLocker ,AES, SHA-256 Hash, RSA Signed  (HIPAA Recommended for Windows OS) **Data in Storage (Server):** TwoFish  (An advanced AES system applicable to MySQL Databases)  **Data in Transit:** CISCO AES-CTR | **TPM-** Hardware that stores signed root cert for three main networks  **2FA** –Toopher authentication for all payments to outside partners  **CISCO ACL**  **Inner Firewall** -  IP Black/White lists |
|  | **Accessing User / Provider Data:**  ePHI Services Performed Provider/ User IDs | **Data in Storage (Device):** BitLocker ,AES, SHA-256 Hash, RSA Signed  (HIPAA Recommended for Windows OS) **Data in Storage (Server):** TwoFish  (An advanced AES system applicable to MySQL Databases)  **Data in Transit:** CISCO AES-CTR  Kerberos Authentication Realm 3 PKI/Digital Certificate Signing(PGP) CISCO AES-CTR / VPN | **TPM-** Hardware that stores signed root cert  **2FA** –Toopher authentication for all payments to outside partners  **CISCO ACL**  **Inner Firewall** -  IP Black/White lists |
| **Remote Corporate Workers** | Devices connecting from home/work site to Local Corporate Network | **Data in Storage (Device):** BitLocker, AES, SHA-256 Hash, RSA Signed  **Data in Use:** Kerberos Authentication Realm 4 (Best for trusted hosts on insecure network)  **Data in Transit:** VPN, AES 256, RSA | **TPM-** Hardware that stores signed root certs for three main networks  Restrict WPA2 connections Media Sanitization SSDs for Laptops |

### UNDERSTANDING THE Healthcare Ecosystem

****

(Csulak & Meadows, 2017)

# LAWS, REGULATIONS, AND STANDARDS

## Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCIDSS) provides a detailed, 12 requirements structure for securing cardholder data that is stored, processed and/or transmitted by merchants and other organizations (PCI, 2016).

*These steps help validate payment applications used by merchants to process electronic payments. “Validation occurs after payment applications have been assessed for compliance by Payment Application Qualified Security Assessors using the Payment Application Data Security Standard (DSS).”*

Below are the key areas where data needs encryption mechanisms:

| Focus Area | PCI RULE Detail | Section |
| --- | --- | --- |
| WIFI | 2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. | Requirement 2: Do not use vendor supplied defaults for system passwords and other security parameters. |
| Non-Console Admin Access | 2.3 Encrypt all non-console administrative access using strong cryptography. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. | Requirement 2: Do not use vendor supplied defaults for system passwords and other security parameters. |
| Stored Data | 3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. | Requirement 3: Protect stored cardholder data |
| Pin Storage | 3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization | Requirement 3: Protect stored cardholder data |
| Disk Storage | 3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. | Requirement 3: Protect stored cardholder data |
| Document &Protect: Card Data | 3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: Note: This requirement applies to keys used to encrypt stored cardholder data, and applies to key-encrypting keys used to protect data-encrypting. | Requirement 3: Protect stored cardholder data |
| Private Key Storage | 3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: Encrypted with a key-encrypting key that is at least as strong as the data encrypting key, and that is stored separately from the data-encrypting key Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) As at least two full-length key components or key shares, in accordance with an industry-accepted method Note: It is not required that public keys be stored in one of these forms. | Requirement 3: Protect stored cardholder data |
| Document &Protect: Key management | 3.6 Fully document and implement all key-management processes and procedures for  cryptographic keys used for encryption of cardholder data, including the following: Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov | Requirement 3: Protect stored cardholder data |
| Retirement of Keys | 3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes. | Requirement 3: Protect stored cardholder data |
| Strong protocols during transmission | 4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include but are not limited to the Internet Wireless technologies, including 802.11 and Bluetooth Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) General Packet Radio Service (GPR | Requirement 4: Encrypt transmission of cardholder data across  open, public networks |
| Wireless Connection Best Practices | 4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission. | Requirement 4: Encrypt transmission of cardholder data across  open, public networks |
| Documenting Transmission Policy | 4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties. | Requirement 4: Encrypt transmission of cardholder data across  open, public networks |
| (PCI, 2016) | | |

## Health Insurance Portability and Accountability Act (HIPAA)

| HIPAA & RULES | DESCRIPTION | LINK |
| --- | --- | --- |
| Health Insurance and Accountability Act (HIPAA), 1996 | Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. | https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996 |
| Privacy Rule, 2000, Mod. 2002 | This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. | https://www.hhs.gov/sites/default/files/privacysummary.pdf |
| Security Rule, 2003 | This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. | https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html |
| Enforcement Rule, 2006 | Provides standards for the enforcement of all the Administrative Simplification Rules. | https://www.gpo.gov/fdsys/pkg/FR-2006-02-16/html/06-1376.htm |
| EFT Fees and HIPAA | Summary of EFT relates issues | http://www.rcmanet.org/Portals/17/02Resources/Practice%20Resources/EFTFeesandHIPAA.PDF |
| HIPAA Combined Regulation Text | Unofficial version that presents all the HIPAA regulatory standards in one document. | https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf |
| Breach Notification Guidance | The U.S. Department of Health and Human Services (HHS) has helpfully provided a web site with “Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals | http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html |

### Protected Health Information (ePHI):

Electronic Protected Health Information (ePHI) is simplified as health information, demographic information, health care provider, health plan, employer, health care clearinghouse, past present, present, future physical or mental health or condition of an individual.

See [Appendix VI](#EPHI) for a larger list of ePHI Information.  
Link: https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/

### HIPAA Violations

The penalty structure for a violation of HIPAA laws is tiered, based on the knowledge a covered entity had of the violation. The Department of Health and Human Services’ Office for Civil Rights (OCR) sets the penalty based on many “general factors” and the seriousness of the HIPAA violation (HIPAA Journal, 2015).

| CATEGORY | VIOLATION DESCRIPTION | FINE AMOUNT |
| --- | --- | --- |
| CATEGORY 1 | A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules | Minimum $100 per violation up to $50,000 |
| CATEGORY 2 | A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules) | Minimum $1,000 per violation up to $50,000 |
| CATEGORY 3 | A violation suffered as a direct result of “willful neglect” of HIPAA Rules, in cases where an attempt has been made to correct the violation | Minimum $10,000 per violation up to $50,000 |
| CATEGORY 4 | A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation | Minimum fine of $50,000 per violation |

| TIER | PENALTY |
| --- | --- |
| Tier I | Reasonable cause or no knowledge of violation – Up to 1 year in jail |
| Tier II | Obtaining PHI under false pretenses – Up to 5 years in jai |
| Tier III | Obtaining PHI for personal gain or with malicious intent – Up to 10 years in jail |

**Estimated Costs of Violations**

The average breach cost $355.00 per stolen record in the healthcare arena (Snell, 2016). This is over twice the average cost of stolen records for all industries (See appendix I). The Anthem data breach of 78.8 million consumers and a lawsuit costing the insurance firm $115 million (Snell, 2017b). Other costs may involve the hospitals desperate act to receive information encrypted by ransomware.

# CONFIDENTIALITY POLICY

| ENCRYPTION COMPONENT | SPEC SELECTION | GUIDANCE | DATA TYPE |
| --- | --- | --- | --- |
| Transport Layer Encryption | TLS 1.2 | Special Publication 800-52 Revision 1 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations | TRANSIT |
| Block Cipher for Web Server | GCM in TLS 1.2 | NIST SP 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC | TRANSIT |
| Block Cipher for Customer/Provider Data in Storage | CBC random IV for TwoFish | NIST Special Publication 800-38A 2001 Edition Recommendation for Block Cipher Modes of Operation: Methods and Techniques | STORAGE |
| Block Cipher for Bitlocker | CBC for AES | RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec BitLocker: https://cryptoservices.github.io/fde/2014/12/08/code-execution-in-spite-of-bitlocker.html | STORAGE |
| Hash for Short-term (BitLocker) | BitLocker SHA-256 | FIPS 180-4 Secure Hash Standard (SHS)  https://technet.microsoft.com/en-us/security/ff690553.aspx | STORAGE |
| Hash for Long-term (years) | SHA-3 | FIPS PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions | STORAGE |
| Hash for Server Connection | SHA-256 | FIPS 180-4 Secure Hash Standard (SHS) | TRANSIT |
| MAC for LAN & VPN | HMAC-SHA256 | RFC 4868 for HMAC IP Sec FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC) Guide to IPsec VPNs, 800–113, Guide to SSL VPNs | TRANSIT |
| Key Protocol for BitLocker / Internet | RSA 2048 (at least) | NIST Special Publication 800-57 Part 3 Revision 1 Part 3: Application Specific Key Management Guidance | STORAGE /TRANSIT |
| Key Protocol for Web Server | ECDH | RFC 5480 Elliptic Curve Cryptography Subject Public Key Information  NIST Special Publication 800-56A Revision 2 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography | TRANSIT |
| Key Management / Authentication for users of CompanyX database | Kerberos | NIST Best Practices for Privileged User PIV Authentication  Kerberos Configuration https://technet.microsoft.com/en-us/library/cc749438(v=ws.10).aspx | STORAGE / TRANSIT |
| Key Management / Authentication for Communications with Providers/partners | RSA based (“SSL”) certificates | NIST Special Publication 800-57 Part 3 Revision 1 Part 3: Application Specific Key Management Guidance | TRANSIT |
| Employee Devices | FDE App to encrypt boot sequence AES 256, CBC, HMAC SHA256 | NIST Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices | STORAGE |
| Data Disposal | Alterec: Destruction | NIST Special Publication 800-88  Revision 1: Guidelines for Media Sanitization | DISPOSAL |

## HASH & mac fUNCTIONS

Cryptographic hashes safeguard data by providing a secure checksum. The current attributes of a good hash function include the following: 1. Speed, 2. Changing one-bit should change entire hash, 3. Avoid hash collisions (Scott, 2013). Currently, many IT associations like NIST and the OWASP foundation, an open community dedicated to application security, recommends at least SHA-256 or higher for the hash function (OWASP, 2017). Therefore, most of the hashes used will be SHA-256 for simplicity and efficiency. SHA is designed to be used with 128-,192-,256 bit key sizes of AES (one of the main algorithms we will be using) (SHA-256, n.d.). As for MACs, it is recommended by security professionals in the community, and recommended by both NIST and HIPAA to use HMAC SHA-256. HMAC avoids key recovery attacks that reveal K to the attacker, and avoids attacks that can be done by the attacker without interaction with the system (Ferguson, 2010).

|  |  |
| --- | --- |
| **DATA TRANSFERS AND COMMUNICATIONS** | **HASH/MAC USED** |
| * Patient billing and administrative information exchanged with payers and health plans. * Utilization and case management data, including authorizations and referrals that are exchanged with payers, hospitals and utilization management organizations. * Lab and other clinical data electronically sent to and received from outside labs. * Patient billing and administrative information exchanged with payers and health plans * E-mails between physicians and patients, and between attending and referring physicians and their offices | APPLICATION MESSAGES MACED- HMAC-SHA256 |
| * Patient health information gathered from or displayed on a Web site or portal. * Word-processing files used in transcription and other kinds of patient reports that are transferred electronically * Stored Emails, Lab Information, Patient billing information | FILES HASHED SHA256 FROM WEB OR ON DISK |
| (Kibbe, 2005) | |

## Problem: Key Exchange

One of the main supporting controls for the confidentiality policy is the secure transmission and storage of cryptographic keys. Brian Tung, a researcher on key exchanging explains the common key exchange issue: *“The password must transit that network in the clear--that is, unencrypted. That means that anyone listening in on the network can intercept the password, and use it to impersonate the legitimate user. Distorting the password (for instance, by running a one-way hash over it) does no good; so long as identity is established solely based on what is sent by the user, that information can be used to impersonate that user”* (Tung, n.d.).

### Solution: Kerberos Server

The Kerberos server is a key management system to administer the secure allocation of encryption keys. Kerberos is based on the Needham-Schroeder protocol which is a symmetric algorithm to establish a secure connection between two parties on a network. The Kerberos website explains their system as the following: “*Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all their communications to assure privacy and data integrity as they go about their business”* (MIT, 2017). The Kerberos key distribution center (KDC) provides an authentication service (AS) and a ticket granting service (TGS) for clients on the network accessing patient or business information (File servers). Below, I have created a step-by-step summary of the server communication tasks:

### Multiple Kerberos “Realms”

Having one sever maintain all keys provides an obvious security concern. The dependence on a single system for key distribution raises an information security issue of availability since failure at a single source will have devastating effects on the whole network. To mitigate this issue, we will be implementing Kerberos “realms” which are administrative domains for different departments and interfaces (e.g. Remote workers to VPN, Corporate Workers to Corporate Data). “*Each realm has its own KDC, which maintains keys only for those users and servers in its realm. The KDC is now broken up into three logically distinct entities: the AS and TGS, as before, and the remote TGS, which services requests from other realms” (Tung, 2002).*

| REALM # | GROUP |
| --- | --- |
| I | Customers |
| II | Providers / Partners |
| III | Corporate Workers |
| IV | Off-site Employees |

### HYBRID PKI SYSTEM

**VPN & Mobile Solution:** For our PKI platform and software we will be using Citrix due to its historical record for providingthe top 10 largest healthcare organizations in the United States (Citrix, 2017). Our PKI solution will utilize Citrix XenApp & XenDesktop to manage access to applications. Specifically utilizing the Windows Server and XenMobile Server for Symantec Managed PKI (MPKI). Options include the configuration of Azure Active Directory (AD) as the identity provider (IDP) lets users enroll in XenMobile using their Azure credentials. The XenMobile Server must connect to Windows Active Directory (AD) using LDAP. The local LDAP server must be configured to sync with Azure AD (Citrix, 2017). To be HIPAA compliant, the server is required to possess an “X.509 version 3 public key certificate” (Ouellette, 2013). The policy, procedures and security controls are optionally represented in the certificate using the certificate Policies extension, specified in RFC5280 and updated in RFC6818 (Ouellette, 2013).  
  
**Connected Medical Devices:** PKI will play an important role in connected medical devices.Encrypted messages from the medical device can provide assurance that configuration, firmware, and components remain unaltered. For example, the certificates can be used to ensure that software on a wireless infusion pump remain unmodified.

### MANAGEMENT OF KEYS AND CERTIFICATES

**Internal Authority:** For employees or remote workers to obtain certificates, the IT department will confirm with HR the existence of the employee, and will install the digital certificate identifying the user. Users may be identified by the Citrix platforms and Azure AD. Any hardware changes (trusted root) on the device to support the integrity of the PKI system will need to be adjusted by the IT security team.

**External Authority:** The organization will be using Symantec Managed MPKI and SAFE-BioPharma Bridge Certificate Authority (SBCA) to secure identities of organizations operating within and beyond the network. The SAFE-BioPharma organization is a non-profit and provides trust in bridging certificates across the pharmaceutical and healthcare networks. BioPharma describes its purpose as providing *“non-repudiable signatures linked to individual’s proven identity. Guarantees life-long document integrity. Digital signature applications certified compliant with the SAFE-BioPharma standard meet global regulatory and legal requirements”* (SAFE-BioPharma, n.d.).

**Restriction & Revocation:** The application for certificate issuance will require the ability to place restrictions on any sub-CA’s. Without a restriction, all sub-CA’s operate as a master key which would be a faulty design (Ferguson et al., 2010).The keys will be revoked if the users secret key is assumed to be compromised, the user is no longer certified by the CA, or the CA’s certificate is assumed to be compromised (Jung, n.d). Security team will use an authority revocation list (ARL) and certificate revocation list (CRL) to revoked certificates. For new users and devices, the security team removes/revokes old keys and certificates and places new key/certificate using root cert on user’s device *offline*.  
  
**Short lived & Long-lives certificates:** The long-term root certificates in an hardware security module (HSM) will be kept offline, except when it is needed to sign shorter-lived intermediate certificates. The intermediate certificates, stored in an online HSM, can do the day-to-day work of signing end-entity certificates and keeping revocation information up to date (Certificate Authority, n.d.).

## RSA SETUP

RSA in the organization will be used for both encryption and signing messages. Like DH, the p and q are large primes, of equal size, that are used to compute n (n=pq). Additionally, n will be 2048 or 4096 bits depending on how current systems perform. It is recommended that an application package should support values up to 8192 bits long to accommodate security requirements of the future. To avoid a common issue with RSA, short common exponents will be used to allow predictable performance and avoid no solution for “d” (a mechanism to generate the private key). It should be noted that there is no issue with large exponents for security, only for poor padding implementation (D.W., 2011). The exponents will be different to not allow attackers to guess the other exponent in the event if one exponent for a system is revealed. Safeguarding information regarding the private key is crucial. As any one of the values consisting of the private key (p,q,d,t,) allows the attacker to computer the other items. During the RSA key generation process, we will make sure the implementation includes a loop counter to make sure the PRNG does not return the same common result (same pseudo-numbers generated). If possible, any software claiming RSA capability will need a review under the community microscope to make sure it’s implemented correctly.

## THREAT MITIGATION & SUPPORTING CONTROLS

### HEALTCHCARE THREAT SUMMARY

The combined value of a healthcare firm’s data and its connected third parties are a treasure trove for attackers. The databases include a vast amount of personal and contact information in *a sharing* culture to streamline healthcare’s vast ecosystem *(See appendix II)*. It should the concern not only of the hospitals administration, but the US Government to secure these networks. The healthcare industry invests around 6% of their annual budget to cyber security while financial and federal governments invest twice as much (Silverman, 2017). The Ponemon 2016 Cost of Data Breach report showed in 2016 that “*48 percent of all incidents involved a malicious or criminal attack, while 25 percent were caused by negligent employees or contractors (human factor). Finally, 27 percent involved system glitches, including both IT and business process failures*” (Silverman, 2017). The Anthem data breach of 2015 compromising 78.8 million consumers, is reported to be caused by a foreign nation using a phishing email (Snell, 2017a). Bring your own device (BYOD) policies provide greater challenges. Devices using voice commands are prompting security concerns as they are hackable with ultrasonic frequencies called a DolphinAttack (Khandelwal, 2017). The high frequency commands are sent to the device instructing the device to visit malicious websites, spy, inject fake information, carryout DoS, or conceal attacks.

### MINNIMUM CONTROLS

| SUPPORTING CONTROL | CONTROL DESCRIPTION |
| --- | --- |
| Two-Factor Authentication (used for Customer login)  . | Two-factor authentication for VPN (Virtual Private Network) access as an optimal security measure to protect against online fraud and unauthorized access for clients that connect to their networks from a remote location.  **Toopher** – user can use safe zones, where customers don’t need to enter 2FA code or phrase when near their home or work |
| Web Application Firewall (WAF) | Web servers and databases protected from malicious online attacks by investing in a web application firewall (WAF). A network firewall’s open port allows Internet traffic to access websites, but it can open servers to potential application attacks, such as database commands to delete or extract data sent through a web application to the backend database, and other malicious attacks. |
| Vulnerability Scanning | Vulnerability scanning checks the firewalls, networks, and open ports. It can be a web application that can detect outdated versions of software, web applications that aren’t securely coded, or misconfigured networks. To meet PCI compliance, you must run vulnerability scans and produce a report quarterly. |
| Patch Management | If servers are not updated and/or managed properly, the data and applications are left vulnerable to hackers, identity thieves and other malicious attacks against your systems. |
| Antivirus | Antivirus software detects and removes malware to protect data from malicious attacks. |
| (Technical Security, N.D) | |
| NO FTP Connections | Open FTP connections can cause issues on the network (Pham, 2015). |
| TPM | TPM Hardware to seal the volume master key. The volume master key to be protected by the internal hardware component. If an attacker copied the data, they will not be able to unencrypt with a pin/password. |
| Employee Read Policy (Signed off) | Make sure HR has signature of every current and new employee has comprehended policy. |

### Added Cryptographic Mechanism Controls

**Strong Entropy Sources:** Cryptographic package provides inclusion of random data from timing of keystrokes, mouse movements and clicks, network traffic, or all at the same time for the random generator. This prevents the attacker of guessing the random data used in the encryption mechanisms to prevent leaking information regarding old message requests.  **Large Pool for Random Source:** By taking in a large pool of source for random data, it will be difficult for the attacker to enumerate possible values for the random generator

### OPERATING SYSTEM Related CONTROLS

**Hardware and OS Supports fully atomic and permanent file updates**: The location of random bits (entropy) collected by the cryptographic system to seed a random generator will require OS and hardware to support a write to disk file update. Additionally, the file is only accessed by that cryptographic system. This allows the seed file not to be lost in RAM and will prevent attackers from knowing the random mechanism.   
**Superusers:** Users assigned administrative access can access areas on a machine that normal users cannot. These memory areas may be useful to a malicious insider that intends to compromise a cryptographic system. Additionally, they can establish other users or control other data that will create a complex environment that may reveal secrets due to user oversight.  
**OS Reinstalled**: There are numerous reasons to reinstall Windows. In this case, it is obvious that the access to encrypted files will be lost.  
**Incorrect Moving of a User to Another Domain:** If a user was moved improperly, he will be unable to access his encrypted file.  
**User Profile Deleted**: Even if a user with the same name is created, he receives another ID and system cannot decrypt the data.  
**A system administrator or user himself cancelled the password**: Results in the loss of access to EFS-data.

### Hardware & Software Considerations

**Keyboards:** Physically check to make sure keyboards are not tampered with. Prevent theft of credentials by encrypting every keystroke. Anti-keyloggers can protect the clipboard and webcam from being hijacked by malware creators. This anti-key logger will have to be tested that it doesn’t interfere with keyboard drivers, related hardware, or other crypto systems. Additional controls should include hardware to prevent Keyloggers from being installed on the tower. **Virtual memory System Swap Files:** Virtual memory used in Windows to run programs in parallel create swap files that may contain system secrets. Specify certain parts of memory are not to be swapped out. Application and OS should support the configuration of locking memory for certain applications. **Defense Against Cold Boot Attack:** Physical access to memory after a reboot or when drive is physically extracted, can release information regarding cryptographic keys. Using Boojum method can help obscure data of cryptographic key in memory. **Cache:** Data stored in cache memory will be wiped clean. Legitimate versions of CCleaner Professional can help wipe the caches for selected programs. **Debuggers:** Windows processes can be attached to running processes which can read memory. Initialization by an attacker can read secrets. **TPM:** TPM Hardware to seal the volume master key. The volume master key to be protected by the internal hardware component. If an attacker copied the data, they will not be able to unencrypt with a pin/password.

|  |  |  |  |
| --- | --- | --- | --- |
| **Data in Use:** Devices | Device Configuration (e.g. encrypted data on phones) and other configurations to ensure security (PGP, AES,Twofish, etc)) | STIG master List A-Z| & National Checklist Program Repository | USE STIG found on https://iase.disa.mil/stigs/Pages/a-z.aspx USE ISCG found on https://nvd.nist.gov/ncp/repository |

### **NO KNOWN THREATS TO SHA-256**

No current weaknesses identified by the community. SHA family developed by the NSA and considered to be the industry standard. In the event SHA-256 is compromised, we can expect most programs, applications, and connections adjusting to SHA-3., Focus will be on strong encryption algorithms, entropy, and implementation.

### **HMAC-SHA256**

Generic birthday attacks against the functions make use of internal collisions of the iterated hash function (Ferguson at al., 2010). Output of hashes are 2n/2 and a birthday paradox assumes two hashes to match. According to researches, no methodology to break HMAC-256 with a birthday attack are known (Bellare, 2014).

### destruction of stored or recorded media containing phi

Paper, images/film, and hard copy of media will be shredded or destroyed when PHI cannot be read or cannot be reconstructed. Redaction will not be accepted as a means of data destruction.

There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack.

**Disintegration, Pulverization, Melting, and Incineration.** These sanitization methods are designed to destroy the media. They are typically carried out at an outsourced metal destruction or

licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

**Shredding.** Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm2).

**Further Guidance – NIST Special Publication 800-88, Guidelines for Media Sanitization**

### RSA Protocol Threats

The main threat to RSA is due to its mathematical structure. Two digitally signed messages m1, m2 sent to Bob can predict the third message m3 by m3:m1m2 mod n. Another threat is due to small messages where no modular reduction takes place. For example, if m^5, an interceptor can recover the message by taking the fifth root. To avoid the common and advance attacks, we will use “padding” or “encoding” to remove structural issues that RSA relies on.   
  
*“There are security issues about having a small private exponent; a key-recovery attack has been described when the private exponent length is no more than 29% of the public exponent length. When you want to force the private exponent to be short (e.g. to speed up private key operations), you more or less have to use a big public exponent (as big as the modulus); requiring the public exponent to be short may then be viewed as a kind of indirect countermeasure” (Pornin, 2011).***RSA Signature:** A safeguard will be used to avoid the same issue described above regarding “n” being smaller than the HASH size of SHA-256. Again, if n^256\*5 = 2^1280, resulting in m^e = m^5 < n, then no modulo takes place and an interceptor can use a fifth root to decrypt message.

### DH Protocol Threats

The DH protocol by itself does not protect against the man-in-the-middle (MITM) attack. In this type of attack, the interceptor can pretend to be the receiver or sender of the message. To provide a safeguard, the receiver can read back a few digits back to sender to verify they are using the same key. This method is effective when the sender or receiver can guarantee they are communicating with the actual person. Therefore, speech synthesizers pose a threat to the verification system. Further challengers show up from users that are not aware of security complications or the severity of not following protocols.

The MITM can replace g^x and g^y by trading keys with the number 1 and both sender and receiver will end up with key, k =1. With k=1 the encryption protection falls apart. Another issue arises when the interception changes g^x to a smaller sub group. If the set contains only 1 million elements, an interceptor can easily search for the correct key. This method is used in case sender and receiver can check to make sure the key does not equal 1 as mentioned above. To avoid this attack, both sender and receiver must check the numbers they have received do not generate small subgroups.

### CERTIFICATE THREATS

**Forgery:** The primary risk in the system is the forgery of certificates with a stolen private key. The private keys will be stored in a hardware security module (HSM) that allows the signing of the key by prevents extraction of the key with both physical and software controls. Other types of forgery are mitigated by HR communicating with IT for certifying public keys to existing employees and revoking certificates for those no longer at the company. For external parties, the SAFE-BioPharma (no-for-profit) organization will provide bridging authority to identify and trust those parties.

**Expiration:** The second risk is the key being compromised over time. The key strength is related to the common computation power trying to break it. The future may prove to re-encrypt components with stronger encryption schemes as computational power of computers grows over time *(SANS, 2001).* The Confidentiality Policy will explicitly restrict the sharing of sensitive keys/certificates and outline acceptable permissions for key sharing. Therefore, a reasonable expiration date and time will be placed on the certificate according to its use. Workers from an audit firm may need a certificate for a few weeks or months, while remote employees may need certificates on a quarterly or half year basis. Extra attention may be placed on the severity of the healthcare operations and legal issues (e.g. prescriptions issuance, procedure approvals); SANS Institute recommends the following: *“Use certified third-party time stamp services or build and certify your own but the important thing is to have a way to prove that the time service itself is reliable and accurate within a given tolerance” (SANS, 2001).*

**Storage of Keys:** The security team will place special attention on decryption abilities as records in the healthcare industry will need to be retained for decades**.** As media deteriorates or software is upgraded, the security team must insure safe transition and compatibility of PKI software *(SANS, 2001).* An example may include a nesting period is an OS of a key in order for they certificate to be valid (Gutmann, 2000). **TLS Server:** Insecure internet connections to websites may provide false keys and certificates. The TLS protocol will offer up-to-date and competent confidentiality and authorization services (Kambourakis et al., 2005). TLS 1.2 protocol has been required since January 1, 2015.

# CONCLUSION

The consideration of OS and cryptographic controls will incur labor costs during implementation but will result in a strong cryptographic system. The hardware, OS, and software considerations will be difficult to determine without further specifications of the network layout. Most of the costs will be due to updating OS and devices to carry supporting hardware (specifically TPM) to accommodate the latest and most secure cryptographic processes.

**Kerberos & PKI Cross**

For our PKI platform and software, we will be using Citrix due to its historical record for providingthe top 10 largest healthcare organizations in the United States (Citrix, 2017). Our PKI solution will utilize Citrix XenApp & XenDesktop to manage access to applications. Specifically utilizing the Windows Server and XenMobile Server for Symantec Managed PKI (MPKI). Options include the configuration of Azure Active Directory (AD) as the identity provider (IDP) lets users enroll in XenMobile using their Azure credentials. The XenMobile Server must connect to Windows Active Directory (AD) using LDAP. The local LDAP server must be configured to sync with Azure AD (Citrix, 2017). To be HIPAA compliant, the server is required to possess an “X.509 version 3 public key certificate” (Ouellette, 2013). The policy, procedures and security controls are optionally represented in the certificate using the certificate Policies extension, specified in RFC5280 and updated in RFC6818 (Ouellette, 2013).

We established to have a sound authentication system without slowing the system, CompanyX will need a hybrid Kerberos PKI model utilizing Kerberos server, LDAP, and PKI components. PKI resolves the administration issue with customers with keeping track of certificates. The PK-Cross includes:

• Establishment of Kerberos Cross Realm relationships using Public Key

• Mutual Authentication of KDCs

• Secure Generation of Static Keys

(Altman, 2007)

**EFT & TECS Payment Solutions**

With the recent smartcard threat, we will need additional mechanisms to make sure patient data cannot be compromised using pieces of the public key embedded on the payment card (Goodin, 2017). Currently we have selected the following TECS system shown below, but this may need to be placed on hold to see how the vulnerability in smart cards will be resolved.

Version #: 10.000.xx  
App Type: Payment Gateway/ Switch  
Tested Platforms/Operating Systems: Windows Server 2012, CentOS  
Service Pack/Build/Version: SP1, 7.2  
Validated According to PA-DSS (PA-DSS v3.2)

**Surrender Existing 2FA SmartCard System & Implementation of Toopher**CompanyX will have to give up their recent smart card system due to the recent vulnerabilities announced (Goodin, 2017).We evaluated a number of 2FA providers and selected Toopher. They provide the best user experience and GEO location security to locate device to a specific area for authentication. That means accounts payable department offices can be mapped with Toopher and authenticated to along with their geo location before sending payment from CompanyX systems.

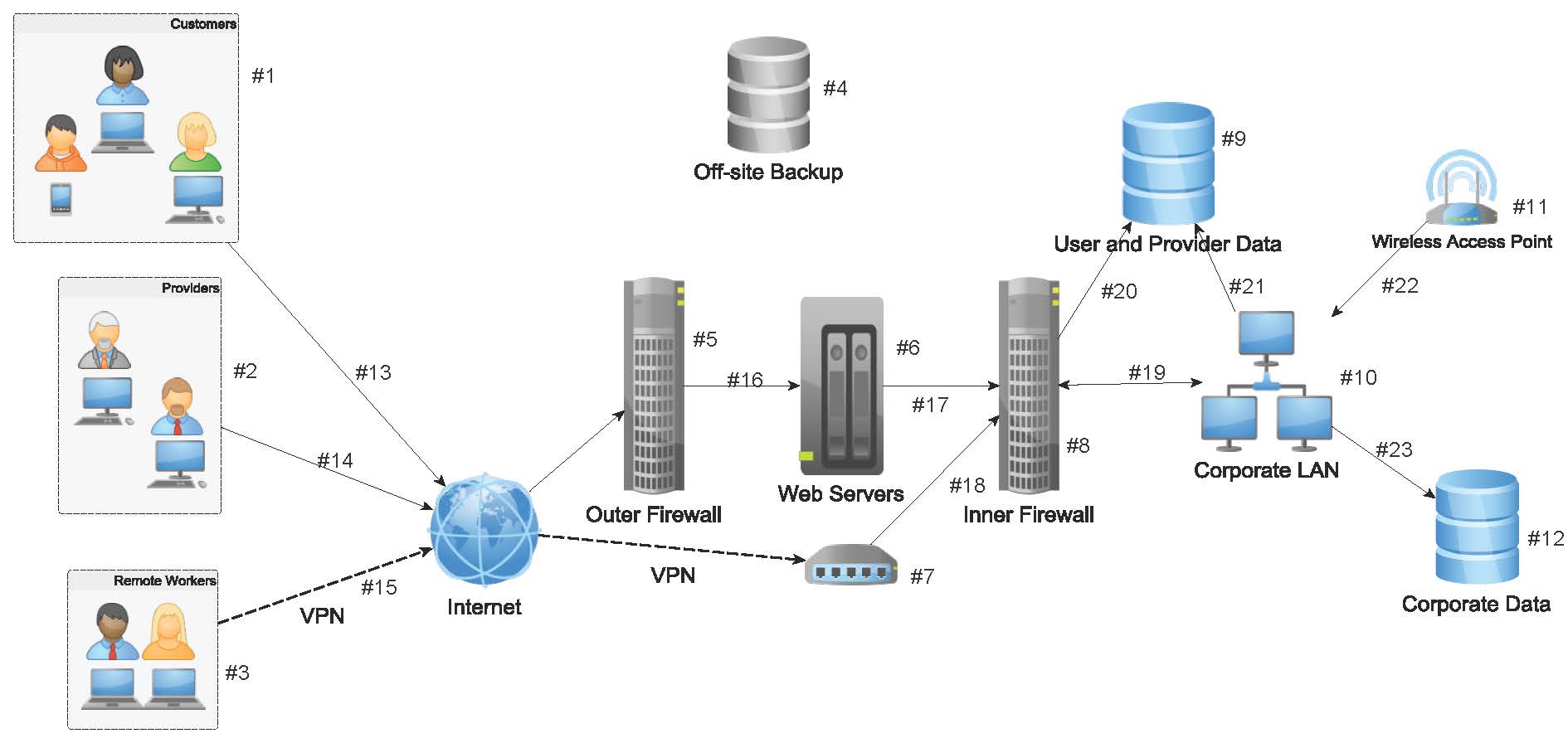
**Securing ePHI Upon Disposal**  
CompanyX currently requires proper disposal of hard disk media. I recommend the Aleratec Hard Disk Drive Demolisher priced at $1,099.90. It is moderately priced and has decent reviews.

**Threat Intelligence Platform**A threat intelligence platform can prioritize vulnerabilities in a wide array of devices operating to be patched by the IT team. This will support the cryptographic architecture by making sure no data leaks are in place.

**TPM COST**The Planning department will need to assess all devices that in network before an estimate of new devices / TPM chips/hardware can be determined.

**ROI  
R**Enhancedencryption technology to protect data will allow lowered price for cyber security insurance and avoid costly lawsuits**.** “Encryption can add nearly 20% to an organizations ROI in security, and render data useless in the event of a breach” (O’Leary et al., 2017).

# APPENDIX I: CRYPTOGRAPHIC diagram



**How to read the table(s) that correlate to the diagram:**

Components and Interfaces **WITH encryption** will have the first row highlighted in blue. Example:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Remote Workers** | **Full Disk Encryption (FDE) - BitLocker** | Algorithm / Block / Key Size | AES / cipher block chaining (CBC) or XTS mode / key 128 or 256 |

Components and Interfaces **WITHOUT encryption** are highlighted in grey (with supporting controls listed). Example:

|  |  |  |  |
| --- | --- | --- | --- |
| **(1) Customers** | **None** | Additional Controls | During registration, make them answer questions or check off ways they can keep their ePHI safe.  Registration for CompanyX services will clearly outline how customer will be contact, and what information would be discussed (Not to give up certain information).  Announcements to customers recommending how to connect securely (e.g. not on public Wi-Fi WPA2) |

## Components

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPONENT** | **ENCRYPT TECHNOLOGY** | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| 1. **Customers** | **None** | Additional Controls | During registration, make customers answer questions or check off ways they will or attempt to keep their ePHI safe.  Registration for CompanyX services will clearly outline how customer will be contacted, and what information will be discussed (Not to give up certain information).  Announcements to customers recommending how to connect securely (e.g. not on public Wi-Fi WPA2) |
|  |  | Threats | Socially engineered customers Connecting on insecure WAPs (Public WIFI) |
| **(2) Providers** | **None** | Additional Controls | During registration, make them answer questions or check off ways they can keep their ePHI safe.  Registration for CompanyX services will clearly outline how customer will be contact, and what information would be discussed (Not to give up certain information).  Announcements to customers recommending how to connect securely (e.g. not on public Wi-Fi WPA2) |
|  |  | Threats | Socially engineered providers Compromise of Provider network |
| 1. **Remote Workers** | **Full Disk Encryption (FDE) - BitLocker** | Algorithm & Block / Mode / Key Size | AES 128 / cipher block chaining (CBC) or XTS mode / Key size 256  This is the options and standard for BitLocker. BitLocker is recommended for institutions to comply with HIPAA regulation. |
|  |  | Hash | SHA-256 BitLocker hashes the user-specified PIN using and the first 160 bits of the hash are used as authorization |
|  |  | Key Protocol | RSA-Volume master key is encrypted |
|  |  | Key Management | **TPM+PIN+USB protectors** TPM-only storage root key. TPM seals volume master key protected by both the TPM and the PIN. To unseal the volume master key, you are required to enter the PIN each time the computer restarts or resumes from hibernation. |
|  |  | Additional Controls | **Minimum Laptop**  Solid State Drive to assist with encryption Patch Management & supported OS 164.308(a)(5)(ii)(B)  Malware Protection (ideally from centralized console) 164.308(a)(5)(ii)(B)  Even though they call this one “addressable, IMO full-disk encryption is a must 164.312(a)(2)(iv) – We recommend AD/Azure with BitLocker full-disk encryption\*, Symantec Endpoint Encryption (PGP), or McAfee Encryption.  Session Idle timers set to lock or logoff 15-30 minutes (depending on your org’s workflows) 164.312(a)(2)(iii)  Disposal and reuse procedures (secure wipe before reuse or destruction for disposal) 164.310(d)(2)(ii)  Device and Media Controls (tracking and remote wipe/lock management if lost or stolen) 164.310(d)(2)(iii) |
|  |  | Threats | Stolen laptop, unauthorized access to data  Access to master keys if BitLocker is implemented incorrectly with TPM  Windows OS issues: reinstallations, improper configuration |

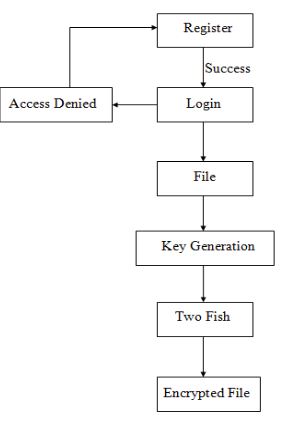
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **COMPONENT** | **ENCRYPT TECHNOLOGY** | | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| 1. **Off-Site Backup** | | **Duel Disk Encryption of backups** | Algorithm & Block / Mode / Key Size | **Duel encryption** AES 128 block/ CBC /Key size 256 Serpent 128 block / CBC / Key size 128 Independent keys for each. Due to the value of the data stored in a database backup, extra encryption will be applied. Since the information does not allow quick access, we can encrypt the data with an extra mechanism to further secure against decryption by adversaries. Serpent is designed for full security and not efficiency  **Can copy data of Cloud Storage using application like Rclone.** |
|  | |  | Hash | SHA-3  Due to the value of the data stored in a database backup, the backups falling in the wrong hands even with encryption can be edited or corrupted in a high-level attack. SHA-3 provides a long-term strategy to authenticate in the case that SHA-2 is compromised. |
|  | |  | Key Protocol | RSA |
|  | |  | Key Management | RSA keys on media protected by bank account/vault by Sec team |
|  | |  | Additional Controls | SOP to securely create backup (e.g. disconnected from network while backup process starts)  SOP and policy for secure transportation of backup data to safe site.  Secure location of file storing hashing of backups Transfers offline using rsync is a utility for efficiently transferring and synchronizing files across computer systems, by checking the timestamp and size of files. |
|  | |  | Threats | Network connected during backup process  Backup script not working  Backup mechanism conflicting with other tasks  Database backups left unprotected during transport (connected online or altered on insecure connection) |
| 1. **Outer Firewall** | | **None** | Additional Controls | 1. Allows connections through the firewall based on source and destination addresses and ports (e.g. IP & Port Blacklist and Whitelist). A proxy firewall adds to the filtering firewall the ability to base access on content either at the packet level or at a higher level of abstraction. 2. SMTP proxy on the firewall collects the mail. It analyzes that email for computer viruses and other forms of malicious logic. 3. Password protected firewall settings. 4. Firewall software updated frequently 5. Encrypted or password protected firewall documentation in word or excel. |
|  | |  | Threats | Enter through the Webserver port (HTTP & HTTPS). The firewall checks for legal, well-formed HTTP(S) requests. Only legal, well-formed HTTPS requests are forwarded to the DMZ Web server.  Enter through the SMTP port. The mail proxy will detect such an attempt and reject such attempts.  Bypass the low-level firewall checks and exploit vulnerabilities in the firewall. The system admin will update the firewall software frequently |

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPONENT** | **ENCRYPT TECHNOLOGY** | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| **(6) Web Server - Public Facing Site** | **HTTPS/TLS 1.2** | Algorithm & Block / Mode / Key Size | AES-128 / GCM / Key 128 (TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_\_SHA256) Galois/Counter Mode (GCM) is a mode of operation for symmetric key cryptographic block ciphers that has been widely adopted because of its efficiency and performance. A fix was released as the Encrypt-then-MAC extension to the TLS specification, released as RFC 7366. The Lucky Thirteen attack can be mitigated in TLS 1.2 by using only AES\_GCM ciphers; AES\_CBC remains vulnerable. |
|  |  | Hash | SHA-256  Used to create the message digest, a cryptographic hash of each block of the message stream. SHA-256 considered more secure than MD5 and SHA-1 used in TLS1 or SSL implementations. |
|  |  | MAC | HMAC-SHA256 |
|  |  | Key Protocol | Elliptic-curve Diffie–Hellman (ECDH) is an anonymous key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel. |
|  |  | Key Management | RSA 2048 Key (recommended as secure, 1024 is not)  1. Server sends a copy of its asymmetric public key to browser.  2. Browser creates a symmetric session key and encrypts it with the server’s asymmetric public key then sends it to the server.  3. Server decrypts the encrypted session key using its asymmetric private key to get the symmetric session key.  4. Server and browser now encrypt and decrypt all transmitted data with the symmetric session key. This allows for a secure channel because only the browser and the server know the symmetric session key, and the session key is only used for that specific session. If the browser was to connect to the same server the next day, a new session key would be created. |
|  |  | Additional Controls | Web server contains only public information that the company wants to distribute. Additionally, no confidential data is ever present on the DMZ Web server.  Any customer data collected is encrypted and stored elsewhere on the server using public key encryption. An SSH connection is used to download that data to an internal server for order processing. By using public key encryption on only the public key would be stored on the Web server. This means that even if an attacker did compromise the DMZ Web server, she would not be able to decrypt the data because she would not have the private key needed for the decryption (Clemson, n.d.). |
|  |  | Threats | Brute force password attempts (restrict with login attempts, password length requirement, and 2FA)  Cross-site scripting (XSS)- to retrieve user credentials  Cross-site request forgery- forwards commands from malicious site to legitimate site.  Malicious HTTPS requests  Path Traversal- Path traversal vulnerabilities can be found when the application allows user-controllable data to interact with the filesystem. |

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPONENT** | **ENCRYPT TECHNOLOGY** | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| 1. **VPN** | **VPN** | Algorithm & Block / Mode / Key Size | AES 128 block /CBC (most commercial applications) /256 key  This AES setup if what most commercial applications provide, and is the standard as recommended on HIPAA websites. |
|  |  | Hash | SHA-256 to authenticate connection. SHA-256 is often the industry standard used by the VPN to authenticate user connection. |
|  |  | MAC | HMAC-SHA256 |
|  |  | Key Protocol | Elliptic-curve Diffie–Hellman (ECDH) is an anonymous key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel. |
|  |  | Key Management | RSA 2048 Key (recommended as secure, 1024 is not) |
|  |  | Additional Controls | SOP needed for process on how to grant access, monitor, and revoke VPN access.  Windows user password |
|  |  | Threats | Unauthorized personnel connecting to hospital network (e.g. stolen laptop, stolen certificate)  Cross-site scripting (XSS) on VPN application - to retrieve user credentials |
| **(8) Inner Firewall** | **None** | Additional Controls | Password protected firewall settings.  Firewall software updated frequently  Encrypted or password protected firewall documentation in word or excel.  Inspection of access logs |
|  |  | Threats | Unauthorized access of hospital data.  Unauthorized changes to network applications and programs that may support cryptographic network  Brute force attempts to files. Mitigated with access attempt logs. |

**(Continued)**

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPONENT** | **ENCRYPT TECHNOLOGY** | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| **(9) User / Provider Data on Server** | TwoFish | Algorithm & Block / Mode / Key Size | TwoFish 128 block / CBC random IV / 256 key  PHI information and provider info encrypted using TwoFish. “Optimized for 32-bit CPUs” (legacy) which are often present at providers. “TwoFish is unpatented, and the source code is uncopyrighted and license-free; it is free for all uses” (Schneier, n.d.) |
|  |  | Hash | SHA-256 |
|  |  | Key Protocol | ECDHE (if available) RSA if more efficient |
|  |  | Key Management | **Kerberos Server for key generation (ticket) and database access Citrix & Symantec MPKI for mobile access** |
|  |  | Additional Controls | 1. Access control matrix (personnel access information needed for tasks) 2. Two-factor authentication (2FA) for user and provider access. 3. Audit or access logs for unusual activity or signs of brute force entries (IT alerts). 4. Preventing access to sensitive information from higher-risk devices, such as mobile devices 5. Configuring the organization’s devices (including desktop computers) to prevent writing sensitive information to removable media, such as CDs or USB flash drives, unless the information is properly encrypted |
|  |  | Threats | Export of user or provide database that includes customer PHI or financial information. Mitigated with IDS and other data protection software.  Failing to encrypt ePHI. Mitigated with manager audits. |
| **(9b) User / Provider Data on Workers Device** | Full Disk Encryption (FDE)- BitLocker | Algorithm & Block / Mode / Key Size | **SEE Component #3** for BitLocker encryption details |



(Devi & Ramya, 2017)

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPONENT** | **ENCRYPT TECHNOLOGY** | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| **(10) Corporate LAN- Cisco** | **LAN:** AES-CTR **Cisco Admin Password:** RSA modulus 1024 | Algorithm & Block / Mode / Key Size | AES 128 / CTR / Key 256 on SSHv2 Connection  Encryption mode is used for the session between the SSH server and client: |
|  |  | Hash | None |
|  |  | MAC | HMAC-SHA2 |
|  |  | Key Protocol | Admin Pass: RSA Modulus 1024 (Cisco standard) |
|  |  | Additional Controls | 1. Details of LAN and architecture documents password protected and encrypted in corporate data (#12). 2. Kept updated in case of personnel or network changes 3. Assets classified and prioritized to provide data protection strategies |
|  |  | Threats | Admin credentials stolen  Theft of assets and/or data |
| **(11) Wireless LAN** | **WPA2 w/ CCMP** | Algorithm | Used for guests ONLY. NOT to be used to access corporate network and data.  AES 128 block / CCMP / 128 Key CCMP is an encryption protocol designed for WPA2 Wireless LAN products that implements the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. Processes using a 128-bit key and a 128-bit block size. Because CCMP is a block cipher mode using a 128-bit key, it is secure against attacks to the 2^64 steps of operation. Generic meet-in-the-middle attacks do exist and can be used to limit the theoretical strength of the key to 2n∕2 (where n is the number of bits in the key) operations needed CCMP (cryptography), 2017). |
|  |  | Hash | HAMC-SHA-1 (HMAC-SHA2 if supported) |
|  |  | Key Protocol | Elliptic-curve Diffie–Hellman (ECDH)  An anonymous key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel. RSA for cert/message encryption |
|  |  | Additional Controls | CCMP recommended configuration and password protected.  Reviewed and tested Wi-Fi Hardware.  Documentation (SOP) encrypted and stored securely. |
|  |  | Threats | Network sniffing on unencrypted traffic. Information accessed through VPN cloud prevents viewing of sensitive information. |
|  |  | EMERGING THREAT | Key Reinstallation Attack (KRACK) several key management vulnerabilities in WPA2, the go to authentication standard in Wi-Fi |

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPONENT** | **ENCRYPT TECHNOLOGY** | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| **(12a) Corporate Data** | TwoFish | Algorithm & Block / Mode / Key Size | TwoFish 128 block / CBC random IV / 256 key  PHI information and provider info encrypted using TwoFish. “Optimized for 32-bit CPUs” (legacy) which are often present at providers. “Twofish is unpatented, and the source code is uncopyrighted and license-free; it is free for all uses” (Schneier, n.d.) |
|  |  | Hash | SHA-256 |
|  |  | Key Protocol | ECDHE (if available) RSA if more efficient |
|  |  | Key Management | **Kerberos Server for server database access Citrix & Symantec MPKI for mobile access** |
|  |  | Additional Controls | 1. Access control matrix (personnel access information needed for tasks) 2. Two-factor authentication (2FA) for user and provider access. 3. Audit or access logs for unusual activity or signs of brute force entries (IT alerts). 4. LAN only access. 5. Configuring the organization’s devices (including desktop computers) to prevent writing sensitive information to removable media, such as CDs or USB flash drives, unless the information is properly encrypted |
|  |  | Threats | Export of user or provide database that includes customer PHI or financial information. Mitigated with IDS and other data protection software.  Failing to encrypt corporate data. Mitigated with manager audits. |
| **(12b) Disk Drive on Workers Device** | Full Disk Encryption (FDE)- BitLocker | Algorithm | **SEE Component #3** for BitLocker encryption details |

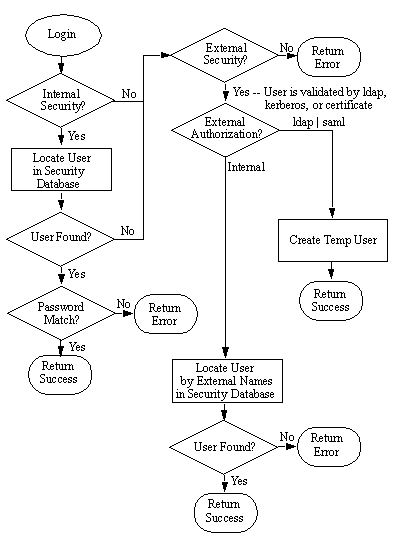
## Interfaces

|  |  |  |  |
| --- | --- | --- | --- |
| **INTERFACE** | **ENCRYPT TECHNOLOGY** | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| **(13) Customers to Outer Firewall** | **None** | Additional Controls | DDOS protections on firewall hardware or ISP service.  Websites / Servers separate between customer and provider traffic. Higher trust in provider related connections Lower trust in customer related connections.  IP black list to filter out possible malicious traffic (IT Security team to research and update blacklist). IP whitelist to clearly identify trusted provider/partner connections. (IT teams communicate on an encrypted channel (e.g. PGP email) regarding changes to network IPs)  The firewall checks for legal, well-formed HTTP(S) requests. Only legal, well-formed HTTPS requests are forwarded to the DMZ Web server. |
|  |  | Threats | Distributed denial of service (DDOS)  IPs from malicious websites  Malicious HTTPS requests. |
| **(14) Providers to Outer Firewall** | **None** | Additional Controls | Threat intelligence platform to provide security stance of business partners. This prevents compromised institution from connecting to network.  Websites / Servers separate between customer and provider traffic. Higher trust in provider related connections. Lower trust in customer related connections.  IP black list to filter out possible malicious traffic (IT Security team to research and update blacklist). IP whitelist to clearly identify provider/partner connections. (IT teams communicate on an encrypted channel (e.g. PGP email) regarding changes to network IPs)  The firewall checks for legal, well-formed HTTP(S) requests. Only legal, well-formed HTTPS requests are forwarded to the DMZ Web server. |
|  |  | Threats | Third-party attack from party on trusted network  IPs from malicious websites  Malicious HTTPS requests. |
| **(15) Remote Workers to VPN** | **None** | Additional Controls | 1. PKI Key transferred to employee offline (LAN ONLY) 2. Updated and secure internet browser when signing to VPN 3. SSH for username/password authentication system to establish a secure connection 4. Two-factor authentication (2FA) or Multifactor authentication (MFA) |
|  |  | Threats | Unauthorized personnel connecting to hospital network (e.g. stolen laptop, stolen certificate)  WPA2 (Krack vulnerability) that can bypass VPN security protocols |

|  |  |  |  |
| --- | --- | --- | --- |
| **INTERFACE** | **ENCRYPT TECHNOLOGY** | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| **(16) Outer Firewall to Webservers** | **None** | Additional Controls | The firewall checks for legal, well-formed HTTP(S) requests. Only legal, well-formed HTTPS requests are forwarded to the DMZ Web server. |
|  |  | Threats | Malicious HTTPS requests. |
| **(17) Web Servers to Inner Firewall** | **None** | Additional Controls | The SSH servicer is configured so that it only accepts connects from the trusted internal admin host. |
|  |  | Threats | Misconfigured service forwarding traffic to another host. |
| **(18) VPN to Inner Firewall** | **None** | Additional Controls | VPN authenticates active user (IT to remove users no longer working or need VPN access)  Firewall whitelist of VPN connections (Backed up and checked regularly against a hardcopy of valid VPN connections) |
|  |  | Threats | Unauthorized access to VPN network. Firewall blacklist/whitelist altered. |
| **(19) Inner Firewall to LAN** | **None** | Additional Controls | CISCO Lan hardware permits certain IPs to access certain nodes on network. VPN restricted to access to user and provider data (Corporate data if needed).  Restrict the network traffic that is initiated from the internal network to email to the DMZ mail server. All other traffic from the internal network to the DMZ or beyond is blocked (e.g. IP & Port Blacklist and Whitelist).  Limited SSH traffic to the Web server in the DMZ and limited SSH administrative access to the computers in the DMZ. |
|  |  | Threats | Unauthorized roaming from internal users and remote workers using VPN. Blacklist, whitelist, ACL altered allowing unauthorized users into network. |
| **(20) Inner Firewall to User / Provider Data** | **None** | Additional Controls | SEE Interface above (#19) |
|  |  | Threats | SEE Interface above (#19) |

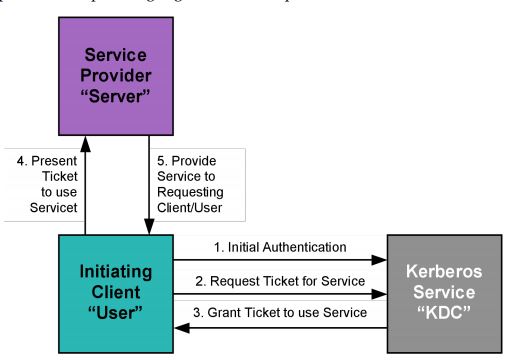
|  |  |  |  |
| --- | --- | --- | --- |
| **INTERFACE** | **ENCRYPT TECHNOLOGY** | **SUBJECT** | **POLICY DETAIL / THREAT MITIGATION** |
| **(21) Corporate LAN to Provider Data** | TwoFish | Algorithm & Block / Mode / Key Size | TwoFish 128 block / CBC random IV / 256 key  PHI information and provider info encrypted using TwoFish. “Optimized for 32-bit CPUs” (legacy) which are often present at providers. “Twofish is unpatented, and the source code is uncopyrighted and license-free; it is free for all uses” (Schneier, n.d.) |
|  |  | Hash | SHA-256 |
|  |  | MAC | None |
|  |  | Key Protocol | ECDHE (if available) RSA if more efficient |
|  |  | Key Management | Kerberos Server for server database access Citrix & Symantec MPKI for mobile access |
|  |  | Additional Controls | Toopher – 2FA – using GPS & word-based authentication. Employees read Confidentiality policy and understand expectations Threat intelligence platform to identify internal threats (Honey pot) OS Controls to make sure cryptographic keys on Windows is not lost or corrupted |
|  |  | Threats | Unauthorized network roaming from VPN or unallocated IPs |
| **(22) WAP for Corporate LAN** | **None** | Additional Controls | WAP (WPA2) will NOT have access to Corporate LAN or Corporate data. |
|  |  | Threats | Unknown remote connections to Wi-Fi (e.g. hidden devices on site, parking lot) |
|  |  | EMERGING THREAT | Key Reinstallation Attack (KRACK) several key management vulnerabilities in WPA2, the go to authentication standard in Wi-Fi |
| **(23) Corp. LAN to Corp. Data** | **LAN:** AES-CTR **Cisco Admin Password:** RSA modulus 1024 | Algorithm & Block / Mode / Key Size | AES 128 / CTR / Key 256  Encryption mode is used for the session between the SSH server and client: Admin Password: RSA modulus 1024 |
|  |  | Hash | None |
|  |  | MAC | HMAC-SHA2 |
|  |  | Key Protocol | ECDHE |
|  |  | Key Management | Kerberos Server for server database access Citrix & Symantec MPKI for mobile access |
|  |  | Additional Controls | 1. Access control matrix (personnel access information needed for tasks) 2. Two-factor authentication (2FA) for user and provider access. 3. Audit or access logs for unusual activity or signs of brute force entries (IT alerts). 4. LAN only access. 5. Configuring the organization’s devices (including desktop computers) to prevent writing sensitive information to removable media, such as CDs or USB flash drives, unless the information is properly encrypted 6. LAN is divided into subnets 7. Admin & routers configurations:   Admin password command: crypto key generate RSA modulus 1024 No HTTP command: no ip http server Access control List (ACL): “ip access-list standard SSH-ADMIN” |
|  |  | Threats | Insider threat exporting of corporate data and financial information. Mitigated with IDS and other data protection software.  Failing to encrypt corporate data. Mitigated with manager audits. |
|  |  | EMERGING THREAT | Smartcards are vulnerable to cloning. Corporate/ employee credit card threat. (Goodin, 2017) |

# APPENDIX II: Authentication BY LDAP, KERBEROS, OR CERTIFICATE



(MarkLogic, n.d.)

# APPENDIX III: kerberos simplified

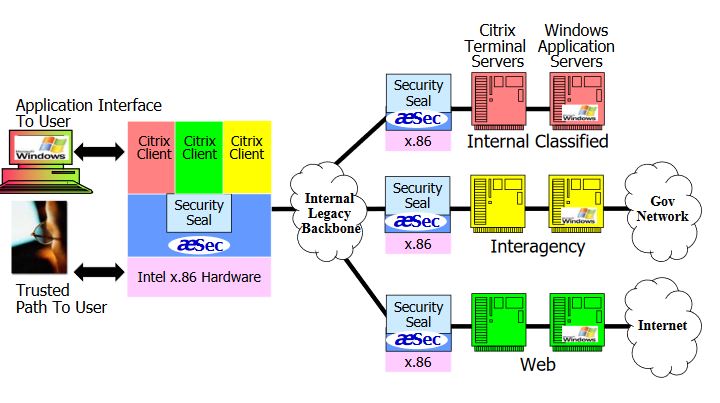


(MIT Kerberos Consortium, 2008)

**Kerberos Steps**

|  |  |  |
| --- | --- | --- |
| **STEP#** | **NODE** | **TASK** |
| 1 | Client | Creates an authenticator using data within device (e.g. device data, time). Portions are unencrypted to communicate with Kerberos server (KDC). Portions are encrypted with user password. |
| 2 | KDC | Matches client device to existing profile using decryption key. The AS on the KDC proceeds to encrypt with own key and transmits back to client. |
| 3 | Client | Stores key in area of memory called Kerberos tray. This area is temporary and never swapped to disk to prevent theft of keys from memory attacks. |
| 4 | Client\* | Submits request to access file server. Access requires ticket from KDC. |
| 5 | File Server\* | Accepts requests from client if valid ticket is presented from client.  Denies request or redirects traffic to the KDC TGS to obtain a valid ticket (continues steps 6-9 presented below) |
| 6 | KDC | Receives request to access file server. Authenticates user by decrypting key provided and loaded to client’s Kerberos tray (key is good for 8 hours by default). Then provides new key (ticket) to client to establish connection on file server. |
| 7 | Client | Receives ticket from KDC and stores in Kerberos tray. The client continues to make request to file server. |
| 8 | File Server | Authenticates client using ticket provided by the KDC. Client granted access to files. (Jones, 2012) |
| \*Cross-Department / “Cross-Realm” Communication: If the user attempts to communicate with information out of their current realm, an extra step is added. The user contacts the AS to authenticate to the local KDC TGS. Then he contacts the KDC TGS to authenticate to the remote KDC TGS. Then the user contacts the remote KDC TGS to authenticate to the end server. The two realms: the user's realm and the server's realm share a cross-realm key, which is used for just this one purpose. The ticket given to the user by the TGS is encrypted with this key, and the remote TGS uses it to decrypt the ticket and authenticate the user (Tung 2002). | | |
|  | | |

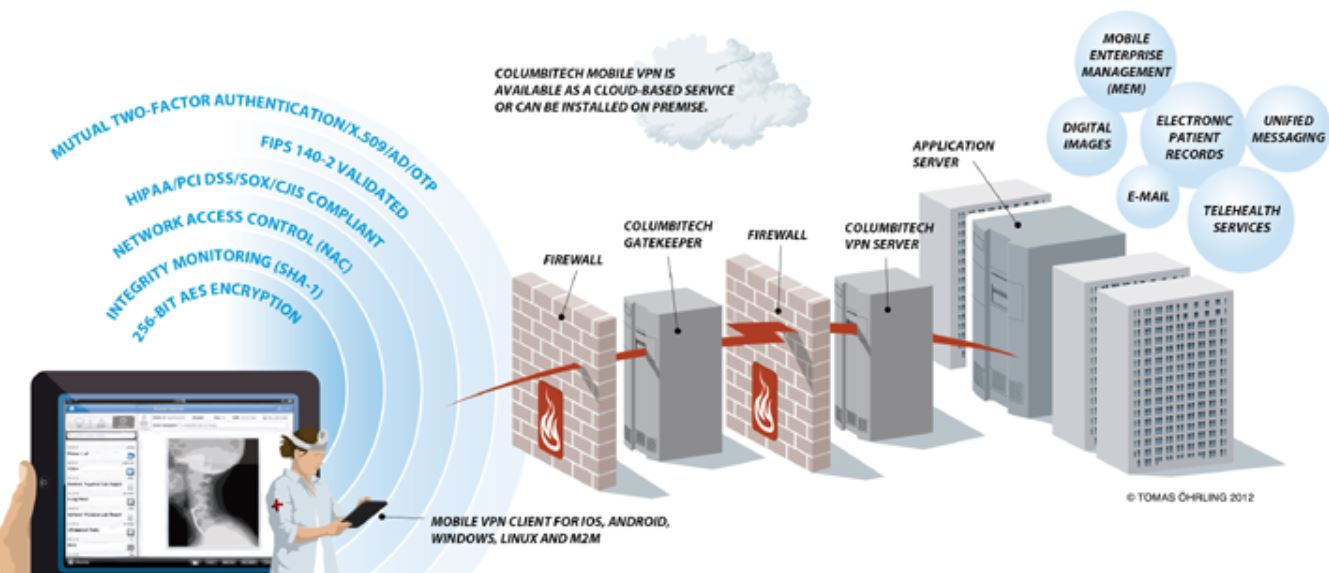
# APPENDIX IV: CITRIX & HARDWARE (EXample: Aesec) IMPLEMENTATION



Aesec is displayed here as the hardware security module to ensure protection of the key/certificates.

(Aesec, n.d.)

# APPENDIX V: EXAMPLE NETWORK to show when VPN/SECURITY is ACCESSED

****

(Columbitech, n.d.)

The network provides secure viewing and record export by using 2FA authentication and connection to the VPN server. Interface traffic to or through firewalls should be encrypted once secure connection is established.

# APPENDIX VI: WHAT DOES PHI INCLUDE?

(2) (i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Censue:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date,, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

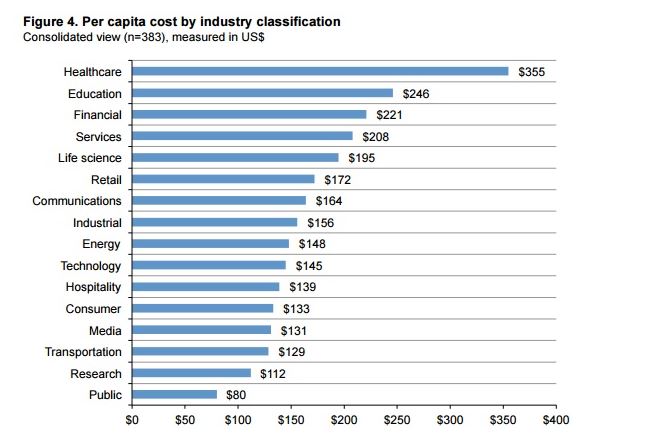
(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(HIPAA, 2017)

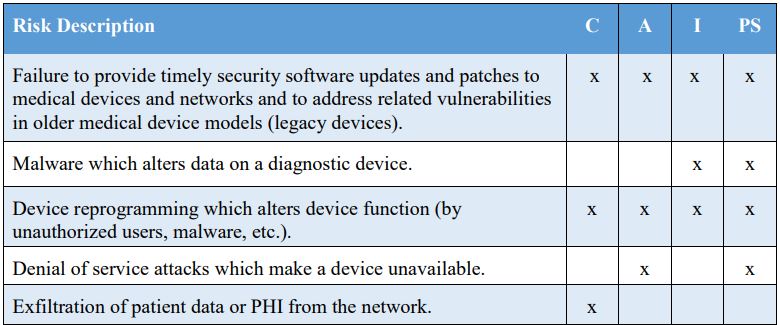
# Appendix VII: Cost of Data Brach per Industry



(Snell, 2016)

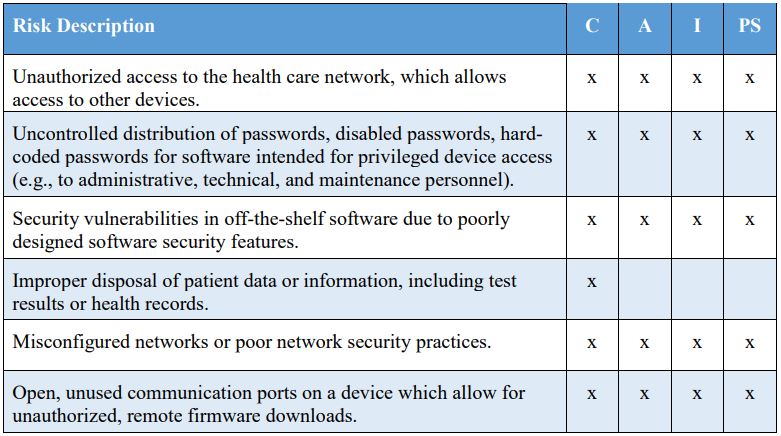
# **APPENDIX VIII: RISK DESCRIPTIONS for DEVICE**

**C=Confidentiality A=Availability I=Integrity PS=Patient Safety**

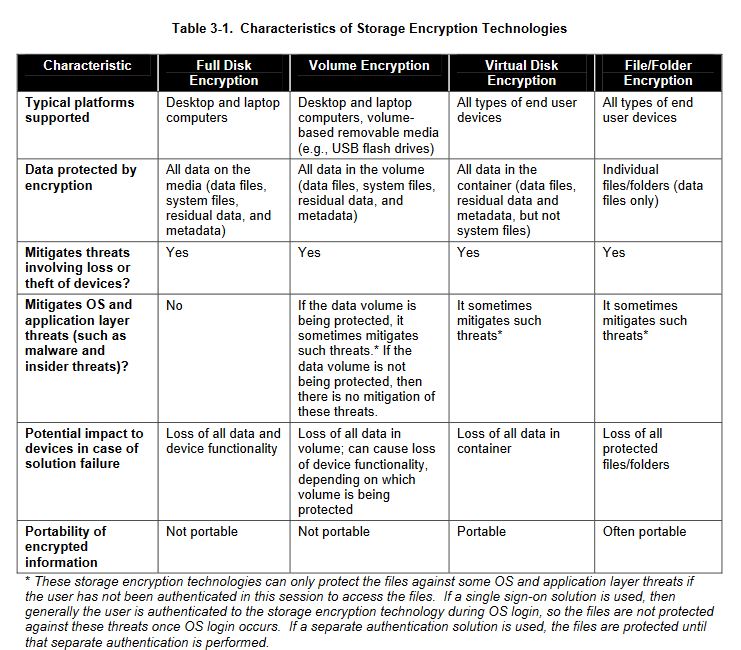
****

# **APPENDIX IX: RISK DESCRIPTIONS for NETWORK**

**C=Confidentiality A=Availability I=Integrity PS=Patient Safety**

****(Csulak & Meadows, 2017)

# Appendix X: Storage Encryption Technologies

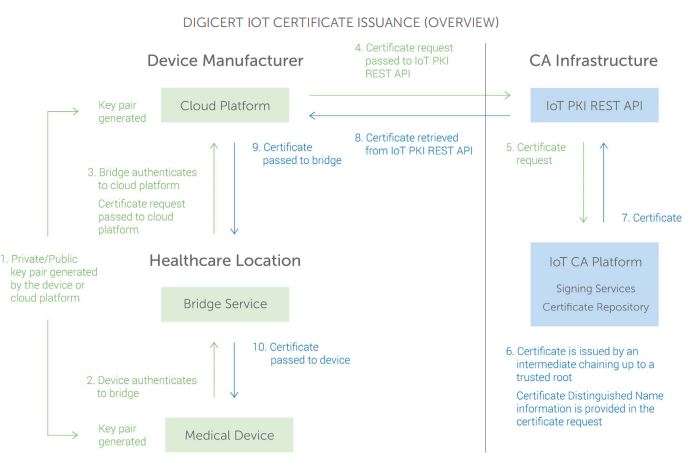
****

(NIST, 2007)

# Appendix XI: PKI OVERVIEW

|  |  |
| --- | --- |
| **PKI SECURE MESSAGE SUMMARY- SIMPLIFED** | |
| **Entity** | **Step Detail (Applicable to PGP for Windows)** |
| Sender | Generate Private/Public Key Pair |
| Sender | Sends public key via secure channel (e.g. trusted link, phone call verification, fax) |
| Receiver | Verifies public key is from intended party and signs/certifies with own key |
| Receiver | Loads the sender’s public key into application and assigns key to recipient |
| Receiver | Creates message and encrypts with sender’s key; transmitted as ciphertext |
| Sender | Receives encrypted message; decrypts with private key (option using a passphrase for added protection) |
| Sender & Receiver | Manages security, expiration, of key and certificates using a secure key managing application |

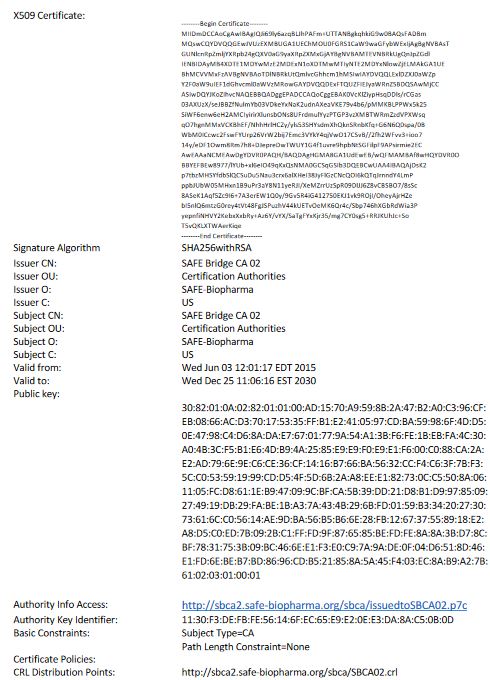
\*Detailed steps (SOP) will be provided for applications approved and implemented into architecture.



(Nelson & Nordenberg, 2017)

Healthcare poses more challenges with PKI due to the various manufactures and devices on-site. Therefore, staff dedicated to the certificates on IoT devices will be needed.

# APPENDIX XII: SAFE-BioPharma Certificate Excerpt



(Safe -BioPharma, n.d.)

# APPENDIX XIII: Acronym Definition

|  |  |
| --- | --- |
| **ACCRONYM** | **DEFINITION** |
| AC | Authentication Service (Kerberos component) |
| CSP | Credential Service Provider |
| FICAM | Federal Identity, Credential and Access Management |
| HTTP | Hypertext Transfer Protocol |
| ICAM | Identity, Credential and Access Management |
| KDC | Key Distribution Center (Kerberos component) |
| LAN | Local Area network |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| RFC | Request for Comment |
| SAML | Security Assertion Markup Language |
| SSHv2 | Secure Shell version2 (SSHv2) session between the server and the client. |
| SSL | Secure Socket Layer |
| TBD | To Be Determined |
| TGS | Ticket Granting Service (Kerberos component) |
| TGT | Ticket Granting Ticket (Kerberos component) |
| TLS | Transport Layer Security |
| TM | Token Manager |
| URL | Uniform Resource Locator |
| VPN | Virtual private network |
| XML | eXtensible Markup Language |

# REFERENCES

Altman, J. (2007, April). NIST PKI’06:Integrating PKI and Kerberos. Secure-endpouints.com. Retrieved from https://www.secure-endpoints.com/talks/nist-pki-06-kerberos.pdf

American Medical Association. (2014, June 20). *EFT Fees and HIPAA*. Rcmanet.org. Retrieved from http://www.rcmanet.org/Portals/17/02Resources/Practice%20Resources/EFTFeesandHIPAA.PDF

Bellare, M. (2014, April). New Proofs for NMAC and HMAC: Security without Collision-Resistance. iacr.org. Retrieved from https://eprint.iacr.org/2006/043.pdf

Certificate authority. (n.d.). *In Wikipedia*. Certificate authority Retrieved October 16, 2017, from https://en.wikipedia.org/wiki/Certificate\_authority

Cisco. (n.d.). *Configuration Examples for AES-CTR Support for SSHv2*. Cisco.com. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\_usr\_ssh/configuration/15-sy/sec-usr-ssh-15-sy-book/sec-aes-ctr-ssh-v2.pdf

Cisco. (2015, August 23). *How to enable AES-CTR encryption for ASA 5520.* Cisco.com. Retrieved from https://supportforums.cisco.com/t5/firewalling/how-to-enable-aes-ctr-encryption-for-asa-5520/td-p/2387325

Citrix. (2017a, September 6). *Azure Active Directory as IDP*. Citrix.com. Retrieved from https://docs.citrix.com/en-us/xenmobile/server/authentication/microsoft-azure.html

Citrix. (2017b, October 2). *PKI Entities*. Retrieved from https://docs.citrix.com/en-us/xenmobile/server/authentication/pki-entities.html

Clemson. (n.d.). *Architecture*. Clemson.edu. Retrieved from https://www.cs.clemson.edu/course/cpsc420/material/Case%20Study/Network/Architecture.pdf

Columbitech. (n.d.). *Wireless Security in Healthcare: Improving care while protecting patient data.* columbitech.com. https://columbitech.com/industry-solutions/healthcare/  
  
Cybersafe. (2015, March 2). *Transparent encryption: pros and cons.* Cybersafesoft.com. Retrieved from http://cybersafesoft.com/blog/transparent-encryption-pros-and-cons-of-the-recovery-mode

Csulak, E., Meadows, T. (2017, June). *REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY.* phe.gov. Retrieved from https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Devi, A., Ramya, B.S. (2017, May 5). *Two fish Algorithm Implementation for lab to provide data security*

*with predictive analysis.* Irjet.net. Retrieved from https://www.irjet.net/archives/V4/i5/IRJET-V4I5754.pdf

Goodin, D. (2017, October 23). *Crippling crypto weakness opens millions of smartcards to cloning*. Arstechnica.com. Retrieved from https://arstechnica.com/information-technology/2017/10/crippling-crypto-weakness-opens-millions-of-smartcards-to-cloning/

D.W. (2011, March 2). *Should RSA public exponent be only in {3, 5, 17, 257 or 65537} due to security considerations?* [Web log post]. Retrieved from https://security.stackexchange.com/questions/2335/should-rsa-public-exponent-be-only-in-3-5-17-257-or-65537-due-to-security-c

Elliptic-Curve\_Diffie. (n.d.). *In Wikipedia*. Retrieved October 3, 2017, from https://en.wikipedia.org/wiki/Elliptic-curve\_Diffie%E2%80%93Hellman

Ferguson, N., Schneier, B., Kohno, T. (2010). *Cryptography Engineering, Design Principles and Practical Applications*. Indianapolis, IN: Wiley Publishing, Inc.  
  
Groza, L. (2001). *Public Key Infrastructure Issues in an Academic Healthcare Setting.* Sans.org. Retrieved from https://www.sans.org/reading-room/whitepapers/vpns/public-key-infrastructure-issues-academic-healthcare-setting-741

HIPAA Journal. (2015, June 24). *What are the Penalties for HIPAA Violations?* Hipaajournal.com. Retrieved from https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

HIPAA. (2017). *HIPAA ‘Protected Health Information’: What Does PHI Include?* Hipaa.com https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/

Hudek, T. (2017, April 20). *AES-CCMP.* Microsoft.com. Retrieved from https://docs.microsoft.com/en-us/windows-hardware/drivers/network/aes-ccmp

*IBM. (n.d.). Kerberos (KRB5) authentication mechanism support for security.* IBM.com. Retrieved from https://www.ibm.com/support/knowledgecenter/en/SSAW57\_8.0.0/com.ibm.websphere.nd.doc/info/ae/ae/csec\_kerb\_auth\_explain.html#csec\_kerb\_auth\_explain\_\_kerbdoub

Jones, D. (2012, October 11). *MicroNugget: View How Does Kerberos Work?* [Video Log]. Retrieved from https://www.youtube.com/watch?v=RICaMlGWopA

Jones, E. (2009, July 14). *Transmission Security Encryption: What to Do and How to Do It.* Hipaa.com Retrieved from https://www.hipaa.com/transmission-security-encryption-what-to-do-and-how-to-do-it/

Jung, E.J. (n.d.). *Public Key Infrastructure (PKI) and Pretty Good Privacy (PGP)*. Usfca.edu. Retrieved from http://www.cs.usfca.edu/~ejung/courses/686/lectures/08pki.pdf

Kambourakis, G., Maglogiannis, I., Rouskas, A. (2005, January 1). *PKI-based Secure Mobile Access to Electronic Health Services and Data.* Retrieved from https://content.iospress.com/articles/technology-and-health-care/thc00388

Kelly,S., Frankel, S. (2007, May). *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec.* IETF.org. Retrieved from https://tools.ietf.org/html/rfc4868

Khandelwal, S. (2017, September 6). *Hackers Can Silently Control Siri, Alexa, & Other Voice Assistants Using Ultrasound.* Thehackernews.com. Retrieved from http://thehackernews.com/2017/09/ai-digital-voice-assistants.html

Khandelwal, S. (2017, September 7). *Shadow Brokers Leaks Another Windows Hacking Tool Stolen from NSA’s Arsenal*. Retrieved from http://thehackernews.com/2017/09/shadowbrokers-unitedrake-hacking.html

Kibbe, D.C. (2005, April). *Ten Steps to HIPAA Security Compliance.* aafp.org. Retrieved from http://www.aafp.org/fpm/2005/0400/p43.html

*Needham–Schroeder protocol*. (n.d.). In *Wikipedia*. Retrieved August 9, 2017, from https://en.wikipedia.org/wiki/Needham%E2%80%93Schroeder\_protocol

Marco, S. (2015, August 28). *6 Laptop Security Basics*. hipaaone.com. Retrieved from http://www.hipaaone.com/6-laptop-security-basics/

MarkLogic Community. (n.d.). *External Security*. marklogic.com. Retrieved from https://docs.marklogic.com/guide/security/external-auth

Messer, J. [Professor Messer]. (2014, September 19). *Kerberos – CompTIA Secrurity+ SY0-401: 5.1* [Video File]. Retrieved from https://www.youtube.com/watch?v=VpBCJ8vS7T0

Microsoft. (2012, March 22). *Windows BitLocker Drive Encryption Frequently Asked Questions.* technet.microsoft.com. Retrieved from https://technet.microsoft.com/en-us/security/ff690553.aspx

MIT Kerberos Consortium. (2008*). Why is Kerberos a credible security solution*? Kerberos.org. Retrieved from http://www.kerberos.org/software/whykerberos.pdf

Nelson, M. Nordenberg, D. (2017, January 10). *Public Key Infrastructure: A Trusted Security Solution for Connected Medical Devices*. Digicert.com. Retrieved from https://www.digicert.com/wp-content/uploads/2017/04/Whitepaper\_PKI\_ATrustedSecuritySolutionForConnectedMedicalDevices1-10-17.pdf

O’Leary, D., Nelson, J., Green, P., Grahn, A. (2017, March 28*). 7 Key Elements of a Successful Encryption Strategy*. Forsythe.com. Retrieved from http://focus.forsythe.com/articles/364/7-Key-Elements-of-a-Successful-Encryption-Strategy

Onlinetech. (n.d.). *Technical Security*. *Onlinetech.com.* Retrieved from http://www.onlinetech.com/compliance-security/secure-hosting/technical-security

Opentext. (2013, November 6). *How Digital Certificates Help Ensure the Security of EDI Data*. Opentext.com. Retrieved from https://blogs.opentext.com/how-digital-certificates-help-ensure-the-security-of-edi-data/

Ouellette, P. (2013, October 18). *Encrypting healthcare data in motion: NIST TLS best practices*. Healthitsecurity.com. Retrieved from https://healthitsecurity.com/news/encrypting-healthcare-data-in-motion-nist-tls-best-practices

OWASP. (2017). *Guide to Cryptography.* Owasp.org. Retrieved from https://www.owasp.org/index.php/Guide\_to\_Cryptography

PCI Security Standards. (n.d.). *VALIDATED PAYMENT APPLICATIONS*. Pcisecuritystandards.org. Retrieved from https://www.pcisecuritystandards.org/assessors\_and\_solutions/payment\_applications?agree=true

PCI Security Standards. (2016). *The Prioritized Approach to Pursue PCI DSS Compliance.* Pcisecuritystandards.org. Retrieved from https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI\_DSS-v3\_2.pdf?agreement=true&time=1505631382031

Polk, T., McKay, K., Chokhani, S. (2014, April). *NIST Special Publication 800-52 Revision 1. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.* NIST.gov. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Pham, T. (2015, December 7). *Encrypting Data to Meet HIPAA Compliance [Web Log Post]*. Onlinetech.com. Retrieved from http://resource.onlinetech.com/encrypting-data-to-meet-hipaa-compliance/

Pornin, T. (2011, March 1). *Should RSA public exponent be only in {3, 5, 17, 257 or 65537} due to security considerations?* [Web log post]. Retrieved from https://security.stackexchange.com/questions/2335/should-rsa-public-exponent-be-only-in-3-5-17-257-or-65537-due-to-security-c

Public key infrastructure. (n.d.). In *Wikipedia*. Retrieved October 16, 2017, from https://en.wikipedia.org/wiki/Public\_key\_infrastructure

Rouse, M. (n.d.). *Electronic protected health information (ePHI).* techtarget.com. Retrieved from http://searchhealthit.techtarget.com/definition/electronic-protected-health-information-ePHI

Safe-BioPharma. (n.d.-a). *Overview*. Safe-BioPharma.org. Retrieved from https://www.safe-biopharma.org/overview.html  
https://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt

Safe-BioPharma. (n.d.-b). *SAFE-BioPharma Trusted List*. Safe-BioPharma.org. Retrieved from https://www.safe-biopharma.org/assets/SAFE-BioPharma%20Trust%20List%20Human%20Readable.pdf

Scarfone, K., Souppaya, M., Sexton, M. (2007, November*). Guide to Storage Encryption Technologies for End User Devices. Recommendations of the National Institute of Standards and Technology.* Nist.gov. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

Scott, T. [Computerphile]. (2013, November 8). *Hashing Algorithms and Security – Computerphile [Video File].* Retrieved from https://www.youtube.com/watch?v=b4b8ktEV4Bg

Schneier, B. (n.d.). TwoFish. [Web Log Post]. Schneier.com. Retrieved from https://www.schneier.com/academic/twofish

Silverman, L. (2017, July 16*). Hospitals Face Growing Cybersecurity Threats.* NPR.org. Retrieved from http://www.npr.org/sections/health-shots/2017/07/26/539290596/hospitals-face-growing-cybersecurity-threats

Snell, E. (2016, June 16). *Healthcare Data Breach Costs Still Highest Among Industries.* Healthitsecurity.com. Retrieved from https://healthitsecurity.com/news/healthcare-data-breach-costs-still-highest-among-industries

Snell, E. (2017a, January 9). *Anthem Data Breach Reportedly Caused by Foreign Nation Attack.* Healthitsecurity.com. Retrieved from https://healthitsecurity.com/news/anthem-data-breach-reportedly-caused-by-foreign-nation-attack

Snell, E. (2017b, June 26). *$115M Settlement Proposed in Anthem Data Breach Case*. Healthitsecurity.com. Retrieved from https://healthitsecurity.com/news/115m-settlement-proposed-in-anthem-data-breach-case

Stephen. (2013, February 5). *Encrypted offsite backups - where to store the encryption key? [Web Log Post].* Serverfault.com. Retrieved from https://serverfault.com/questions/475441/encrypted-offsite-backups-where-to-store-the-encryption-key

Toopher. [Toopher]. (2014, August 27). *Toopher - Invisible 2 Factor Authentication* [Video File]. Retrieved from https://www.youtube.com/watch?v=IeQp1WU1o0Q

Transport Layer Security. (n.d). *In Wikipedia.* Retrieved on October 23, 2017 from https://en.wikipedia.org/wiki/Transport\_Layer\_Security

Tung, B. (n.d.). *Morons Guide to Kerberos.* Wpollack.com. Retrieved from https://wpollock.com/AUnixSec/MoronsGuideToKerberos.htm

Tung, B. (2002). *Kerberos: Where did it come from and why?* Retrieved from http://web.archive.org/web/20071213045222/http://www.isi.edu:80/~brian/security/why\_kerberos.html

Vanshanu, R. ( 2047, November 17). *21 Years Old Vulnerability Kerberos Dubbed Orpheus’ Lyre – Patch Is Now Developed For Both Windows, Mac & Linux Distros* [Web Log Post]. Technicalbud.com. Retrieved from http://technicalbud.com/2017/07/kerberos-dubbed-orpheus-lyre-security-flaw/

Vengadapapurvaja, A.M., Nisha, G., Aarthy, R., Sasikaladevi, N. (2017, October 16). *An Efficient Homomorphic Medical Image Encryption Algorithm*. Sciencedirect.com. Retrieved from http://www.sciencedirect.com/science/article/pii/S1877050917319798