Enterprise Key Management Policy

Name: PHILOMINA DORKENOO

Date: 1-18-2022

**Policy Statement**

This policy statement, in conjunction with the company-wide key management system overhaul outlined in the Key Management Plan, will establish secure and uniform procedures and practices across all SHC offices branches and locations. Moving to a centralized key management administration allows for more flexibility. Putting these new policies into action and enforcing them corporate-wide in order to close any gaps in our key management safety The Health Insurance Portability and Accountability Act of the United States. SHC is required by law to comply with set security standards in order to protect customers under the Health Insurance Portability and Accountability Act (HIPAA). Health Information That Is Safe (PHI). This policy summarizes the requirements for purposes of protecting and encryption keys that are held by the end users.

**Responsible Executive and office**

The ultimate responsibility for implementing and enforcing this policy rests with the Chief Information Security Officer and the Key Management Administration team, both of which report to him

**Entities Affected by this Policy**

This policy applies to any encryption keys issued by SHC, used for SHC business, and/or used to access SHC systems. With the exception of public keys used in digital certificates, protect SHC-owned information. All employees who have access to the SHC network must follow these policies and complete the required training as per the institution.

**Procedures**

All symmetric (secret) keys in transit must be protected by a key algorithm that is more powerful than the one used by the distributed key. The security of the keys is prioritized over the security of the data encrypted by those keys. The central administration stores all system-wide secret keys in a single location, using specialized hardware security modules that are physically separated from the data servers that they encrypt. All system-wide secret keys must be rotated every six months, along with an audit. All endpoint devices that access and store PHI must use Full-Disk Encryption and be protected by a user-only 8-digit PIN. When an employee leaves the company, the PIN must be disclosed to the property management team so that the storage drives can be wiped and the device re-used.

**Public Key Infrastructure**

Employees who have network access are given a pictured, smart ID card that they must use to access their computers, emails, the SHC internal website, company Wi-Fi, and SHC internal networks via Virtual Private Networking. The smart cards will contain private keys that users will use for digital certificates, and they will require an 8-digit PIN to be entered before they can be accessed. When the Certificate Authority issues the digital signature to the user, the public key is provided to the Certificate Authority. Lost or stolen smart cards must be reported immediately to the security office, and the card's digital certificate must be revoked from the system before a new card with a new public-private key pairing can be issued. Employees who are leaving the company must return their card to be destroyed, and the card's certificates must be revoked from the system by the end of the next business day.

**Training**

All employees who are given a smart card must go through initial training as well as an annual refresher course.

**Enforcement**

Employees who violate this policy may face disciplinary action, including dismissal.