COUNTY OF IMPERIAL
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES

POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA - Encryption	**PROCEDURE:** 01-164
SECTION: Administration	**EFFECTIVE DATE:** 6-8-16
REFERENCE: 45 C.F.R. Subtitle A, Subchapter C, Part 164	**PAGE:** 1 of 6
	SUPERSEDES: New Procedure
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	**APPROVED BY:** Andrea Kuhlen

PURPOSE: To establish a procedure for the encryption of data at rest on fixed and mobile computing devices as well as in inter-application transmissions.

NOTES: This document is applicable to all devices and applications that encrypt and decrypt PHI. It is not applicable to devices or applications that process only encrypted or unencrypted ePHI. It specifies procedures for installation, monitoring, key management and recovery.

The PHI Inventory identifies all of the applications and devices that this procedure addresses.

DEFINITIONS: None

PROCEDURE OWNER: Security Officer

PROCEDURE:

PERSON RESPONSIBLE:	**ACTION:**
	Data at Rest
	Installation:
System Technology Staff	1. Installs Sophos Safeguard at

System Technology Staff (cont.)

prep time.

Note: The system will encrypt the volume after reboot. All files in disk will be encrypted. The encryption is transparent to the user. The software operates transparently, the user has no interaction.

2. Encrypts desktops using the following specifications, Systems:

   a. Vendor - Sophos Safeguard Enterprise Version 7

   b. Encryption Algorithm: FIPS 1490-2 validated cryptography (Attachment A)

   c. Key Management - Pre-shared key certificate with combination domain, user, password

   d. External encryption system components - Sophos Safeguard Enterprise console, Safeguard client, Enterprise Key Ring

NOTE:
Key / Key Recovery
Only domain administrators have access to the enterprise console. None have access to actual encryption key. The application provides a challenge/response mechanism to recover access to the device.

System Technology Staff (cont.)

Monitoring:

> NOTE: Sophos Safeguard provides a reporting tool to monitor access and status of the encrypted device.

Removal:

Systems Analyst

3. Follows the Sophos Safeguard removal procedure included in Attachment B

ICBHS Asset Inventory

Information Systems Staff

ICBHS Asset Inventory includes a data field that labels an asset if encrypted. Reports are run against the database to ensure that assets are labeled.

Data in Transmit

Data Exchange with DHCS / ITWS Website

ICBHS Staff Needing to Send Information to DHCS

1. Identify the file that needs to be uploaded to ITWS website.

> NOTE: There several different types of data that is submitted to ITWS Website including: claims files, Client Service Information (CSI) files, California Outcomes Measurement System (CalOMS)and others.

2. Use the following technology specifications to encrypt the file:

ICBHS Staff Needing to Send Information to DHCS (cont.)

a. Vendor – WinZip

b. Encryption Algorithm: AES 1 and AES 2

c. Key Management – User password

d. External encryption system components – None

NOTE: All files uploaded or downloaded from ITWS are WinZip and encrypted with a password preset by DHCS for each county. DHCS mandates the password to be used on the encrypted file. WinZip is installed and removed by Systems Technology staff according to the request of ICBHS Managers / Supervisors.

3. Select the content of the WinZip file to be encrypted and use the file name and password according to DHCS specifications.

4. Select the content of the WinZip file to be encrypted and use the file name and password according to DHCS specifications.

5. Monitor that the files submitted to ITWS are properly named, properly encrypted, have passed the requirements and a positive file submission message has been received.

Cisco Registered Envelope Services (CRES)

To send ePHI through an email:

ICBHS Staff Needing to Send Information Through an Email

1. Access the following URL for CRES: https://res.cisco.com/websafe/login.action

   The service uses the following technology specifications:

   a. Vendor - CISCO

   b. Encryption Algorithm: Arc-4

   c. Key Management - Managed by Cisco Servers @ Cisco Cloud

   d. External encryption system components - Cisco Iron

Note: NOTE: Any emails that contain electronic protected health information should use CRES. The key is kept by the user who has set up password for assign user name. The CRES service is available through a website service that user signs in to send emails. Email notifications are received in regular emails and website needs to be accessed and credentials entered to have access to the encrypted data. CRES provides a reporting tool to monitor access and status of the users of the encryption services.

ICBHS Staff Needing to Send Information Through an Email (cont.)

2. At the login screen enter county email address and password. Once in the website, under Compose Message, enter the recipient and write the message. The service allows including attachments to the message. Load attachment as needed.