COUNTY OF IMPERIAL
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES

POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA - PHI Protection	**POLICY:** 01-232
SECTION: Administration	**EFFECTIVE DATE:** 10-14-15
REFERENCE: 45 CFR Sections 164.312(c)(1), 164.312(c)(2), 164.312(d), 164.312 (e)(1), 164.312(e)(2)	**PAGE:** 1 of 7 **SUPERSEDES:** New Policy
AUTHORITY: Behavioral Health Director as the Local Mental Health Director/Alcohol and Drug Administrator	**APPROVED BY:** Andrea Kuhlen

PURPOSE: To define the measures that must be in place at ICBHS to protect the confidentiality, integrity and availability of electronic protected health information (EPHI).

NOTES: This policy covers electronic or digital PHI. Hardcopy and other forms of PHI are covered separately.

DEFINITIONS: Availabililty: is defined in the Security Rule, at Section 164.304 as "the property that data or information is acccessible and useable upon demand by an authorized user."

Confidentiality: is defined in the Security Rule, at Section 164.304 as "the property that data or information is not made available or disclosed to unauthorized persons or processes.

EPHI - Electronic Protected Health Information: refers to any protected health information (PHI) that is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulation and is produced, saved, transferred or received in an electronic form.

Integrity: is defined in the Security Rule, at Section 164.304 as "the property that data or information have not been altered or destroyed in an unauthorized manner."

"Mobile Device" and "media" includes CD, DVD, Flash, USB drives, memory sticks, floppy disks, SD card, PDAs, smartphones, tablets and all other technologies that store data in a form that can be moved or transported physically.

Protected Health Information (PHI): Individually identifiable information relating to past, present, or future physical or mental health condition of an individual, provision of health care to an individual, or the past, present, or future payment for health care provided to an individual transmitted or maintained in any form or medium including oral, written, or electronic communication.

Out-of-band: Out-of-band key exchange refers to the use of a completely different medium such as telephone or fax to exchange a passphrase or key.

Server: A computer device on a network that manages network resources.

Workstation: An electronic computing device, for example, a lap or desk computer, or any other device that performs similar functions, an electronic media stored in its immediate environment.
telephone or fax to exchange a passphrase or key.

POLICY OWNER: Security Officer

POLICY: Electronic protected health information (EPHI) must be handled at all times in accordance with the requirements of the Health Insurance and Portability and Accountability Act (HIPAA). HIPAA requires covered entities to "allow access only to those persons or software programs that have been granted access rights as allowed by the HIPAA Privacy Rule"and "implement technical security measures to guard against unauthorized access to electronic protected health information" during transmission and to "implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

Inventory: An inventory of all PHI collected and held by the organization will be developed and maintained. This encompasses paper and other tangible records and the PHI processed and stored in the department's IT devices.

Access: The access to PHI shall be granted only as necessary to conduct activities permitted in the HIPAA Privacy Rule (45 CFR Section 164 Subpart E). The administration of access rights to PHI shall be governed by Policy 01-231, Access Control.

Access Record: A record of all access to client PHI shall be logged and retained in accordance to the HIPAA Privacy Rule (45 CFR 164.528).

Configuration: All devices shall be configured to limit access to EPHI to authorized users using authenticated credentials and access authorization based on roles. Configurations shall be monitored and administrative access logged.

Transmission: All PHI must be encrypted during storage and transmission beyond the perimeter of ICBHS' networks using an encryption protocol meeting industry standards, with keys or passphrases that meet the standards required the ICBHS' Policy 01-100, Passwords and User Identification (ID) Control. All PHI that is physically transported out of any facility must be encrypted unless prior, explicit authorization has been granted by the ICBHS Security Officer.

Storage: Approved locations to store and manage PHI for use by authorized personnel will be identified. Storage of PHI on workstations and laptops shall be strictly limited to temporary files needed by the electronic health record and other applications that process PHI.

Mobile Media: PHI should always be encrypted on mobile media. See Policy 01-235, Mobile Device and Media Security.

Destruction: All media containing PHI, whether encrpyted of unencrypted, must be disposed of before being sold, discarded or repurposed.

Loss: Loss or theft of any device containing PHI, including servers, routers, workstations, laptops, mobile device, and mobile media, whether encrypted or not, must be reported to the Security Officer immediately. Failure to make a report within one (1) hour of discovery is a violation of policy and may result in action under Policy 01-60, Sanctions for Violations of the Privacy Rule and Security Rule.

Standards

1. All devices that store PHI and applications that process PHI shall be accounted for in an inventory of PHI. It shall include:

   * Workstations and laptops (both local to network and remote)
   * Mobile computing devices (including, but not limited to, smartphones, PDAs, tablet computers, etc.)
   * Network attached storage devices
   * Mobile storage devices (including USB flash drives, thumb drives, etc.)
   * External servers or computing infrastructure (cloud-based systems, storage applications, etc.)
   * Backup devices or media
   * Media (CDs, DVDs, etc.)
   * Printers, multifunction devices and fax

2. All PHI stored, archived or held by the organization shall be recorded and tracked in an inventory of PHI that includes records in both tangible and digital or electronic form.

3. All devices and applications shall meet the following required configuration:

   * User sessions shall be locked after 20 minutes of idle connection and terminated after 90 idle minutes
   * Administrative use shall be logged.
   * Changes to system and application configurations shall be logged including the settings:
     * Password
     * Audit Log

4. All PHI is encrypted through Sophos safeguard:

   * The following approved encryption protocols are standards for using, storing and transmitting PHI on across the networks:
     - Symmetric Key: AES, 3DES, and Skipjack
     - Asymmetric Key: DSA, RSA, and ECDSA
     - Secure Hashing: SHA-1, SHA-256 and SHA-512

   * The following protocols are approved for establishing secure transmission across networks

and sharing keys:
- HTPPS
- SSL/TLS
- SSHv2
- IPSEC

5. **Destruction:**

* All media including hard disk drives, CD/DVD or floppy disk, flash memory or thumb drives, print media, and bar or QR codes used to hold PHI must be completely erased before any repurposing within the department.
* Resale or other transfer of media to parties outside the control of ICBHS is prohibited.
* Before disposal, all magnetic (e.g. hard drives, floppy disk) and optical media (e.g. DVD, CDR) must be effectively and wholly destroyed, rendering them unreadable.
* This standard applies to all PHI whether or not it has been encrypted.
* Prior to disposal, printer, faxes, copiers, multi functional devices, network equipment, servers, workstations, laptops, smartphones, and any other devices that could store data and are used to store, transmit, or access EPHI must be analyzed to determine an acceptable disposal method that cannot result in prohibited disclosure of EPHI.

6. **Mobile Media:**

* (See the Mobile Media and Media Security Policy for media standards)

7. **Approved Storage:**

* The following is the list of approved storage locations for PHI held by ICBHS:

Physical Locations:
- Deputy Directors office - Locked cabinets
- Managers offices - Locked cabinets
- Supervisors offices - Locked cabinets
- Medical Records rooms - Locked cabinets
- Staff offices - Locked cabinets
- Medical Records rooms - Locked cabinets

Electronic Locations:
- Avatar application

- Desktops - Encrypted
- Laptops - Encrypted
- Network shared directories

8. **Access Records:**

* Each application that allows users to create, read, update or delete PHI must be configured to create a log each access.
* Access logs must be collected and retained for the purpose of meeting patient requests for a period of seven (7) years.

Related Policies and Regulations:

Policies:

01-100	Password and User Identification (ID) Controls
01-231	User Access Management
01-235	Mobile Device and Media Security Policy
01-247	Malicious Software

Regulations:

1. 45 CFR Section 164.312(c)(1) Standard: **Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
2. 45 CFR Section 164.312(c)(2) Implementation Specification. **Mechanism to authenticate electronic protected health information** (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
3. 45 CFR Section 164.312(d) Standard: **Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
4. 45 CFR Section 164.312(e)(1) Standard: **Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
5. 45 CFR Section 164.312(e)(2) Implementation Specifications: (i) **Integrity controls** (Addressable). Implement security measures to ensure that electronically transmitted

electronic health information is not improperly modified without detection until disposed of.
(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Also see the HIPAA Privacy Rule 45 CFR Section 164.502