


**COUNTY OF IMPERIAL  
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES**

**POLICY AND PROCEDURE MANUAL**

<b>SUBJECT:</b> HIPAA - Mobile Device and Media Security	<b>POLICY NO:</b> 01-235
<b>SECTION:</b> Administration	<b>EFFECTIVE DATE:</b> 10-18-21
<b>REFERENCE:</b> 45 C.F.R. Sections 164.310 (d) (1), 164.310 (d) (2) (iii)	<b>PAGE:</b> 1 of 6
<b>AUTHORITY:</b> Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	<b>SUPERSEDES:</b> 10-14-15
	<b>APPROVED BY:</b> 

**PURPOSE:** To establish the controls that must be implemented to ensure that EPHI stored and transported on storage devices and removable media is appropriately controlled and managed.

**NOTES:** None

**DEFINITIONS:**

**Encryption:** means the use of an algorithmic process to transform data into a form in which there is low probability of assignment meaning without use of confidential process or key.

**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.

**Minimum Necessary:** refers to the least amount of PHI needed to accomplish the intended purpose of the use or disclosure.

**"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.

**Workforce**: In Section 160.103 of the HIPAA Privacy Rule, the "workforce" is defined as "employees, volunteers, trainees and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."

**POLICY Owner:**

Security Officer

**POLICY:**

All devices including mobile devices and mobile storage accessing data, media, networks or storing, reading, writing, transmitting or receiving ICBHS PHI must be approved before being connected to the local network and transmitting or receiving data from it.

The transfer of use of mobile media to store or transport PHI should be kept to an absolute minimum and discouraged except where absolutely necessary.

Mobile devices must be managed in such a way as to protect PHI from unauthorized access and use. Storage media must be either 1) physically secured on the organization's premises, 2) encrypted using an approved encryption process, or 3) "signed out" in a process the records destination of the media, the person who will ensure it is secure and date on which it is returned or destroyed. Any user who transfers PHI to a mobile device or physical transport medium takes full responsibility and

accountability for its secure handling and ultimate disposal. Loss of any device containing PHI must be reported to the information systems manager immediately. The PHI Protection Policy covers loss or theft of media and mobile devices that contain PHI.

**1. Device and Media Protection**

ICBHS shall protect all the hardware and electronic media that contain EPHI. This includes, but is not limited to, workstations computers, laptops, personal digital assistants (PDAs) such as smartphones, USB drives, backup tapes, and CDs.

ICBHS is responsible to develop procedures that govern the receipt and removal of hardware and electronic media that contain EPHI outside of the secured physical perimeter of an ICBHS facility. Procedures shall include maintaining a custody record of hardware and electronic media.

**2. Portable Media Security**

EPHI that is placed in portable electronic media shall be encrypted so that access to the EPHI can only be attained by authorized individuals with access to the decryption code.

Workforce members shall limit the quantity of EPHI on portable electronic media to the minimum necessary for the performance of their duties.

All workforce members shall have permission from their supervisor before transporting EPHI outside of the secured perimeter of an ICBHS facility. Approvals shall include the time period for authorization, which shall be a maximum of one year.

Workforce members shall not leave portable media that contain EPHI visible in their vehicles or any other unsecured location.

If portable media is lost, workforce members are responsible to immediately notify their supervisor.

### **3. Electronic Media Disposal**

Before electronic media that contains EPHI can be disposed, the following actions shall be taken on devices used by the workforce:

- a. Hard drives shall be destroyed to prevent recognition or reconstruction of the information.
- b. Storage media, such as backup tapes, USB flash drives and CDs, shall be physically destroyed (broken into pieces) before disposing of the item.

### **4. Electronic Media Reuse**

All EPHI shall be removed from hard drives when the equipment is transferred internally from one workforce member to another workforce member who does not require access to the EPHI, or transferred externally from ICBHS to another County department. Hard drives shall be wiped clean by IT before transfer.

All other media shall have all the EPHI removed (the mechanism may vary depending in the media type) and tested to ensure the EPHI cannot be retrieved. If the media is not "technology capable" of being cleaned, the media shall be overwritten or destroyed.

### **5. Device Maintenance and Repair**

When the technology is capable, all EPHI shall be removed from the device's memory or hard drive. All other media shall have all the EPHI removed before the device is accessed for maintenance or sent out for repair. Devices include computer servers and any other device capable of storing electronic data.

### **6. Policy Responsibilities**

1. Supervisor and Manager Responsibilities

- ❖ Ensure that only workforce members whose duties require the need to transport EPHI outside of the secured physical perimeter of an ICBHS facility are granted permission to do so.
- ❖ Enforce procedures to govern the receipt and removal of hardware and electronic media that contain EPHI outside of the secured physical perimeter of a County facility, and the movement of these items within the facility.

## 2. IS Support Responsibilities

- ❖ Ensure that only all hard drives are destroyed before disposal, or wiped clean of EPHI before reuse, or sent out for repair.
- ❖ Maintain an inventory and record any movement of hardware and electronic media such as workstation computers, servers, or backup tapes.

## 3. Workforce Members Responsibilities

- ❖ Follow the procedures that govern the receipt and removal of hardware and electronic media that contain EPHI.
- ❖ Limit the quantity of EPHI on portable electronic media to the minimum necessary to perform their duties.
- ❖ Secure EPHI on portable electronic media through encryption.
- ❖ Remove and destroy all EPHI from portable electronic media when it is no longer needed to perform their duties.
- ❖ Do not leave or store portable media that contain EPHI in their vehicles or in any other unsecured location.

**Related Policies and Regulations:**

Policies:

1. PHI Protection Policy
2. Remote Access and Wireless Policy
3. Configuration Policy

Regulations:

1. 45 C.F.R. Section 164.310 (d)(1): Standard: Device and media controls. Improvement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
2. 45 C.F.R. Section 164.310 (d) (2) (iii): Accountability (Addressable). Maintain a record of the movements of hardware, electronic media and any person responsible therefore.