


**COUNTY OF IMPERIAL  
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES  
POLICY AND PROCEDURE MANUAL**

<b>SUBJECT:</b> HIPAA - Physical Security	<b>POLICY NO:</b> 01-291
<b>SECTION:</b> Administration	<b>EFFECTIVE DATE:</b> 6-10-16
<b>REFERENCE:</b> 45 C.F.R. Subtitle A, Subchapter C, Part 164	<b>PAGE:</b> 1 of 6
	<b>SUPERSEDES:</b> New Policy
<b>AUTHORITY:</b> Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	<b>APPROVED BY:</b> 

**PURPOSE:** To ensure that the facilities of ICBHS are maintained in a secure state to protect the PHI that is transmitted, stored, created and otherwise processed on the premises.

**NOTES:** This policy covers the physical infrastructure including locks, doors, windows, etc. and the location of IT components within the facility.

**DEFINITIONS:** **Encryption:** Scrambling or encoding electronic data to prevent unauthorized access or use. Only individuals with knowledge of a password or key can decrypt (unscramble) the data. Encryption methods use an algorithmic process that transforms the data into a form in which there is a low probability of assigning meaning to it without the use of a confidential process or key.

**ePHI:** Protected health information (PHI) that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

**ICBHS:** Imperial county Behavioral Health Services

**Protected Health Information (PHI):** PHI is health information that a covered entity creates or receives, that identifies an individual, and relates to:

- The individual's past, present, or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to the individual.

PHI includes written, spoken and electronic forms. PHI is "individually identifiable information". PHI excludes individually identifiable information in education records, school health records covered by FERPA (Family Educational Rights and Privacy Act), employment records held by a covered entity in its role as employer, or records regarding a person who has been deceased for more than 50 years.

**POLICY OWNER:** Purchasing Unit and Information Systems Behavioral Health Managers

**POLICY:** Access to the facilities of ICBHS shall be regulated by a Physical Security Plan, which the Security Compliance Officer and/or the Physical Security Manager will draft. The intent of this plan is to specify controlled areas within the facility and who, how and when access shall be granted. It will also identify equipment such as computers, servers, network and mobile devices or media that must be protected in order to meet security and privacy requirements.

All ICBHS facilities, with specific exclusions of the after-hours crisis and referral desk, should be locked, protected and inaccessible, unless authorized, after normal working hours or when a receptionist or front staff is not present. Individual rooms within all ICBHS facilities shall be locked whenever PHI or devices that contain PHI are present and unattended. Personnel may be issued keys for access to secure rooms based on their roles and responsibilities according to the ICBHS Key and Lock Control Policy (01-10). The ICBHS purchasing department is responsible for keeping record of each key assigned. All employees who are issued

keys are responsible for maintaining keys in a safe and secure manner.

No equipment will be present in areas that are accessible to the public, additional precautions will be taken to prevent or mitigate potential theft or misuse of ICBHS equipment. Unattended equipment should not contain unencrypted PHI and all accounts will have a screen locking timeout. Equipment visible from public access areas are to be oriented to discourage unauthorized, incidental viewing as required by the HIPAA Privacy Rule.

All fixed and mobile computing systems that access data of ICBHS will be secured against unauthorized access, loss, tampering or theft. Fixed and mobile computing systems include but are not limited to desktop and laptop workstations, servers, firewalls, switches, routers, printers, smartphones, and data ports.

To prevent unauthorized access, publicly accessible fixed and mobile computing systems shall be configured as follows:

- All systems must require login using account and password authentication.
- All equipment must be in a physically secured (locked) location whenever it is unattended.
- Screens must lock and require re-authentication after a period of inactivity.
- Any laptop and mobile device allowed to leave the secured premises should be assigned to one person who must take responsibility to ensure that it is adequately secured at all times to prevent unauthorized access, loss, tampering or theft.
- Loss, tampering or damage of any computing device must be reported to the Security Officer immediately.
- All equipment leaving the facility must meet the encryption standard of the applicable policy.

Transport of PHI into and out of the facility in mobile devices or mobile media is covered in Policy 01-235, HIPAA - Mobile Device and Media Security. Management of hard copy documents containing PHI is addressed in Policy 01-20, Transporting Confidential Client Information.

**STANDARDS :**

1. The Purchasing Unit and Information Systems Behavioral Health Managers shall prepare and maintain a Physical Security Plan that at a minimum covers:
  - The documentation of all fixed IT Equipment that contains PHI
  - Restricted areas within ICBHS facilities
  - Physical Access Control Procedures
  - Procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency
  - Procedures used to grant, maintain and revoke access to the facility and restricted areas
  - Procedures for documenting all maintenance repairs and modifications to the facilities
2. A register of all keys shall be maintained and periodically audited by the purchasing department.
3. All networking equipment must be in locked rooms or enclosures with no access to power switches or other controls except by authorized maintenance personnel.
4. All PHI must be encrypted on any device that is in a publicly accessible or in an uncontrolled area.
5. Reporting of loss, tampering, damage or theft of any equipment must be made to the Security Officer or if not immediately available, to the Information Systems BHM within one (1) hour of detection.
6. Screen locks must be in place to require re-authentication after ninety (90) minutes of inactivity.
7. All IT equipment leaving the facility must be assigned to or checked out to a specific authorized individual.
8. All IT mobile equipment must meet policy requirements for encryption according to the HIPAA Mobile Device and Media Security Policy (01-235).

9. Records must be kept with respect to facility repairs or changes that might affect the physical security of the facility.
10. A periodic physical security review will be performed:
  - Examine past security incidents that have resulted in physical security breaches and assess whether remediation actions have been taken to prevent future incidents.
  - Examine the results of emergency exercises, tests or live drills; identify any weakness or ineffectiveness with respect to controlling facility access during emergencies.
  - For door locks installed in restricted areas, review list of all individuals who process keys and identify those who are not authorized to have keys.
  - If third party facility security is present, validate whether security guards periodically patrol designated areas to monitor suspicious activity based on established procedures.
  - Periodically test door locks and camera surveillance systems to make sure they are functioning as expected.
  - Examine physical protection of computer equipment (desktops and laptops) in offices or in restricted areas.

**Related Policies, Plans and Regulations:**

Policies:

1. 01-232 HIPAA - PHI Protection Policy
2. 01-235 HIPAA - Mobile Device and Media Security Policy
3. 01-231 HIPAA User Access Management Policy

Plans:

1. Facility Security Plan

Regulations:

1. §164.310 Physical safeguards. A covered entity must, in accordance with § 164.306: (a)(1) Standard: **Facility access**

2. §164.310 (a) (2) (ii) **Facility security plan** (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
3. §164.310 (a) (2) (iii) **Access control and validation procedures** (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
4. §164.310 (b) Standard: **Workstation use**. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
5. §164.310 (c) Standard: **Workstation security**. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.