


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

SUBJECT: HIPAA - Workstation Security	POLICY: 01-234
SECTION: Administration	EFFECTIVE DATE: 10-14-15
REFERENCE: 45 CFR Section 164.310(c)	PAGE: 1 of 3
AUTHORITY: Behavioral Health Director as the Local Mental Health Director/Alcohol and Drug Administrator	SUPERSEDES: New Policy
	APPROVED BY: 

PURPOSE: To establish rules for securing workstations that access electronic protected health information (EPHI).

NOTES: Since EPHI can be portable, this policy requires workforce members of HIPAA covered entities to protect EPHI at county worksites and all other locations.

DEFINITIONS: Covered Entity: Under HIPAA, this is a health plan, health care clearinghouse. or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

EPHI: Electronic Protected Health Information. All individually identifiable health information that is created, maintained or transmitted electronically.

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."

Workstation: A computing device, for example, a laptop or desktop computer, or any other device that performs similar functions and any electronic media stored in its immediate environment. 45 CFR 164.304

POLICY: Imperial County Behavioral Health Services (ICBHS) shall implement safeguards to prevent unauthorized access to EPHI through workstations, and to protect EPHI from any intentional or unintentional use or disclosure.

Workstation Security Controls:

All workstations used by workforce members to access EPHI shall be set to automatically lock the computer when it is left unattended, requiring the user to enter a password to unlock the workstation. The standard setting for the computer to lock after a period of inactivity is not to exceed 20 minutes.

Workforce members shall manually lock their workstation computer using the Ctrl-Alt-Delete-Enter keys when the computer is left unattended for any period of time.

Workforce members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and access on computer screens. At each site, every effort shall be made to ensure confidential information on computer screens is not visible to unauthorized persons.

Workforce members who work in facilities that are not HIPAA covered entities, shall be aware of their surroundings to ensure no one can incidentally view EPHI and that no EPHI is left unattended.

Workforce members shall protect printed versions of EPHI that have been transmitted via fax or multi-use machines by promptly removing documents from shared devices.

Workforce members shall place confidential documents in locked cabinets or drawers when left unattended.

Policy Responsibilities

Supervisors and Manager Responsibilities

1. Control workforce member access to EPHI as per Policy 01-231, HIPAA Access Control
2. Take appropriate corrective action if any workforce member knowingly violates the security of workstation use.
3. Ensure that the automatic lock is functioning on all workstations.

4. Ensure that all workforce members are locking their workstation when they are not in use.
5. Ensure that all confidential information is not viewable by unauthorized persons at workstations in offices under their supervision.

Workforce Members Responsibilities

1. Lock their computer when it is left unattended for any period of time.
2. Do not change or disable the automatic inactivity lock on their workstations.
3. Ensure all confidential information in their workstation is not viewable or accessible by unauthorized persons.
4. When working at a non-HIPAA covered entities, protect EPHI from unauthorized access or viewing.

IS Support Responsibilities:

1. When installing new workstations, set the computer to automatically lock after the recommended period of inactivity, which is not to exceed 20 minutes.

Related policies and regulations

Policies:

01-231 HIPAA - Access Control

Regulations

1. 45 CFR Section 164.310(b) Standard: Workstation Use. Implement policies and procedures that specify the proper function and 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.
2. 45 CFR Section 164.310(b) Standard: Workstation Security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.