


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

POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA - Access Control	PROCEDURE: 01-166
SECTION: Administration	EFFECTIVE DATE: 6-8-16
REFERENCE: 45 C.F.R. Subtitle A, Subchapter C, Part 164	PAGE: 1 of 11
	SUPERSEDES: New Procedure
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	APPROVED BY: 

PURPOSE: To provide guidelines for managing access control rights of users within any of the various systems or applications that contain or process EPHI. Among other rights, it sets out procedures for granting, changing and terminating rights based on the user's role in providing services to patients and customers of ICBHS guidelines for implementing security configuration settings on workstations.

NOTES: This document specifies a process to assign functional roles for workforce members, business associates, contractors or other users of ICBHS information technology who have a legitimate need to access EPHI. The functional rules are mapped to access roles that are configured into the applications that contain or process EPHI.

It covers the granting and modifications of access rights to the MyAvatar application that processes EPHI. Workforce members shall ensure compliance with the HIPAA - User Access Management policy prior to obtaining access to ICBHS applications or systems that contain or process EPHI.

DEFINITIONS: Access: The ability of the means necessary to read, write, modify, or communicate data/information or other wise use any system resource.

BHM: Behavioral Health Manager

EHR: Electronic Health Record

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

ICBHS: Imperial County Behavioral Health Services

IS: Information Systems

IS Analyst: Information Systems Analyst is computer systems analyst who works with ICBHS' current computer systems and solutions to help the organization operate more efficiently and effectively

myAvatar: myAvatar is the ARRA-certified electronic health record and practice management application for ICBHS.

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.

ST Analyst: Systems Technology Analyst systems analyst is an information technology (IT) professional who specializes in analyzing, designing and implementing information systems.

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."

PROCEDURE OWNER: Security Officer

PROCEDURE:

PERSON RESPONSIBLE:

ACTION:

User Role Creation:

- | | |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Information Systems
Manager | 1. Consults with ICBHS management for creation of user role and appropriate forms and reports to be associated with user role. |
| Information Systems
Analyst | 2. Creates user role within EHR and documents new user role in User Access workbook. |

EHR Access and User Role Assignment:

- | | |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Office Technician/
Designee | 1. Before access is granted to any of the various systems or applications that contain EPHI, ensures that the workforce members are trained to a minimum standard as outlined in the policy 01-231, User Access Management. |
| Manager/Supervisor | 2. Submits a helpdesk ticket for workforce member's computer and EHR access. |
| Office Technician/
Designee | 3. Submits request to County IT for workforce member's computer access and schedules workforce member's EHR training. |
| | 4. Notifies Supervisor/Manager of scheduled trainings. |

Office Technician/
Designee (cont.)

5. In EHR creates workforce member's credentials and assigns user roles based on workforce member's discipline.

Information Systems
Analyst

6. Provides Security Awareness to workforce member and provides EHR training.
7. Provides workforce member with EHR credentials and ensures workforce member is able to log into EHR.

Note: Prior to being issued a User ID and/or Password to access any EPHI, each workforce member shall sign the Initial Security Awareness Training form and Electronic Signature Agreement.

8. Within 30 consecutive calendar days, shall verify and document workforce member has accessed EHR systems or applications.
 - a. Runs the "No Access in 30 days" report
 - b. If workforce member has not accessed the EPHI system or application, will contact user and supervisor/manager to determine whether access will no longer be required.
 - c. If access is no longer required, will investigate the account to determine if workforce member

Information Systems
Analyst (cont.)

still requires access to EPHI system or application.

NOTE: For business associates, contractors, or other non-workforce members of ICBHS, notification will be provided to IS BHM. BHM will assign IS Analyst to train and document new non-workforce member access to EHR.

Modification of User Roles:

NOTE: Modification of user role will be necessary if a workforce member transfers to another program, workforce member is promoted or demoted, or changes their work role within the same program. The following procedure will be completed upon the need for user role modification.

Manager/Supervisor

1. New program supervisor/manager submits a helpdesk ticket to IS with the following information:
 - a. Workforce member's complete name
 - b. Workforce member's previous and new discipline.
 - c. Effective date of change
 - d. Contact information

Office Technician

2. Assigns helpdesk ticket to IS Analyst.

Information Systems

Analyst

3. Verifies user role access change and makes appropriate user role changes in the EHR.
4. Documents changes in user access workbook.
5. Notifies office technician of completed helpdesk ticket request.

Office Technician

6. Notifies manager/supervisor of completed request and closes helpdesk ticket.

NOTE: For business associates, contractors, or other non-workforce members of ICBHS, notification will be provided to IS BHM. Upon notification, IS Analyst will be responsible for processing and documenting modification of access to non-workforce member account.

Ongoing Compliance for Access:

NOTE: The following consists of steps to ensure that workforce members actively utilizing the EHR.

Information Systems

Analyst

1. To ensure that workforce members are actively utilizing the EHR, run the "No Access in 30 Days" report monthly.
2. If a user ID or logon account that has not been used for more than 30 consecutive calendar days is found,

Information Systems
Analyst (cont.)

will investigate.

a. Notify supervisor/manager and provide a copy of report.

Manager/Supervisor

b. Confirms if workforce member still requires access to EHR.

Information Systems
Analyst

c. Makes appropriate changes to workforce members account.

NOTE: The following consists of steps to ensure that workforce members only have access to specific EPHI within the EHR in accordance to their respective disciplines.

Information Systems
Analyst

1. Quarterly, runs the "Active Assigned Staff User Roles" report.

2. Sends managers or designee a copy of report.

Manager/Supervisor

3. Reviews report and determine if changes in workforce member's user roles are needed.

4. If changes are needed, follows steps described in the **Modification of user roles** section.

NOTE: The following consists of steps Ongoing compliance for access for business associates, contractors or other non-workforce members.

Information Systems

Analyst

1. Runs the "No Access in 30 Days" report monthly for business associates, contractors or other non-workforce members.
2. Provides IS BHM with report.
3. Upon direction of IS BHM, investigate to determine if user account still requires access to EHR.
4. Makes and documents appropriate changes.

Administrative Access Control:

NOTE: Administrator account access is granted and monitored by the IS BHM. The workforce designated as "Administrator" can access EPHI residing in each module of the electronic health record (EHR) application. Access will be reviewed by the IS manager periodically as described in the following steps.

Information Systems

Manager

1. Assigns an IS Analyst to each module of the EHR.

Information Systems

Analyst

2. Maintains and documents changes to the EPHI system or application.

Information Systems

Manager

3. Periodically monitors administrative access and ensures administrative \

Information Systems

Manager (cont.)

accounts are being appropriate used.

4. Completes and documents necessary changes to Administrative user accounts.

Termination or Suspension of Access

A workforce member's access to the EPHI system or application will be removed or deactivated based on the following circumstances.

- A. If management has evidence or reason to believe the individual is using information systems or resources in a manner inconsistent with HIPAA Security Rule policies, access will be terminated immediately.
- B. If the workforce member or management has reason to believe the user's password has been compromised, management will immediately inform IS to suspend account access.
- C. If the workforce member resigns, is terminated, suspended, retires, or is away on unapproved leave from ICBHS.
- D. If the workforce member's or business associate's work role changes and system access is no longer justified.
- E. If the workforce member will be out on temporary leave for more than three weeks, the user account will temporarily be suspended and reestablished upon the workforce member's return to work

Manager/Supervisor

1. If any of the above-mentioned circumstances applies, immediately submits a helpdesk ticket to IS with the following information:

- a. Workforce member's complete name
- b. Workforce member's discipline.
- c. Effective date of termination.
- d. Contact information

Office Technician

2. Verifies with Manager/Supervisor termination date.
3. Deactivates workforce member's account in HER.

Related Policies and Regulations

Policies:

1. 01-128 HIPAA - Audit Controls
2. 01-231 HIPAA - User Access Management

Regulations:

1. 45 C.F.R. Section 164.308 (a) (3) (i): Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.
2. 45 C.F.R. Section 164.308 (a) (3) (ii) (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with

electronic protected health information.

3. 45 C.F.R. Section 164.308 (a) (4) (ii) (C): Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
4. 45 C.F.R. Section 164.312 (a) (1): Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Section 164.308(a) (4).
5. 45 C.F.R. Section 164.312 (a) (2) (i): Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.