COUNTY OF IMPERIAL
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES

POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA – User Access Management	**POLICY NO:** 01-231
SECTION: Administration	**EFFECTIVE DATE:** 6-12-16
	PAGE: 1 of 9
REFERENCE: 45 C.F.R. Subtitle A, Subchapter C, Part 164	**SUPERSEDES:** 10-14-15
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	**APPROVED BY:** Andrea Kuhlen

PURPOSE: To establish rules for authorizing access to the ICBHS network, applications, workstations, and to areas where electronic protected health information (EPHI) is accessible. ICBHS shall ensure that only workforce members who require access to EPHI for work related activities shall be granted access and when work activities no longer require access, authorization will be terminated.

NOTES: None

DEFINITIONS: **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.

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.

Facility: The physical premises and the interior and exterior of a building.

ICBHS: Imperial County Behavioral Health Services

IS: Information Systems

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

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: Only workforce members who require access to EPHI for work related activities shall be granted access and when work activities no longer require access, authorization shall be terminated.

1. **Management and Access Control** - Individual User Account only the workforce member's manager or appropriate designee can authorize access to EPHI information systems. Manager's or their designee are responsible for requesting the appropriate level of access for staff to perform their job function.

Access to the information system or application may be revoked or suspended if there is evidence that an individual is misusing information of resources. Any individual whose access is revoked or suspended may be subject to disciplinary actions or other appropriate corrective measures

2. **Management and Access Control** - Administrator Account Only the workforce designated as "Administrator" can access EPHI residing in each module of the electronic health records (HER). Access is granted by the IS manager. Access will be reviewed by the IS manager periodically. If workforce member no longer requires access, it is the responsibility of the manager or appropriate designee to complete the necessary process to terminate access.

3. **Granting Access to EPHI**

Screen Prospective Workforce Member Prior to Hire
Prior to hire, the following background checks are conducted for each prospective workforce member:

- Department of Justice (DOJ)
  - Criminal Background Check
- Employee Relations, Inc.
  - Verify previous employment information
  - Check DMV Records
  - Verify academic degrees
- Licensing Boards
  - Verify professional licensure
- OIG's List of Excluded Individuals/Entities, United States General Service Administration's System for Award Management (SAM), California Department of Health Care Services Suspended and Ineligible Provider List
  - Verify applicant is not excluded from participation in federal or state funded program
- CalTest
  - Drug testing (clinical staff only)

Screen Workforce Members Prior to Access
The manager or designee shall ensure that information access is granted only after first verifying that the access of a workforce member to EPHI is appropriate.

Security Awareness Prior to Getting Access
Before access is granted to any of the various systems or applications that contact EPHI, the Information Systems staff shall ensure that workforce members are trained to a minimum standard including:

- Proper uses and disclosures of the EPHI stored in the systems or application
- How to properly log on and off the systems or application
- Protocols for correcting user errors
- Instructions on containing a designated person or help desk when EPHI may have been altered or destroyed in error.
- Reporting a potential or actual security breach

Security Acknowledgment
Prior to being issued a User ID or password to access any EPHI, each workforce member shall sign the Initial Security Awareness Training form.

Granting Access in an Emergency
Management has the authority to grant emergency access for workforce members who have not completed the normal HIPAA access requirements if:

1. Management declares an emergency or is responding to a natural disaster that makes client information security secondary to personal safety.

2. Management determines that granting immediate access is in the best interest of the client.

If emergency access is granted, the manager shall review the impact of emergency access and document that event within 24 hours of it being granted.

After the emergency is over, the user access shall be removed or the workforce member shall complete the normal requirements for being granted access.

Termination or Suspension of Access
A workforce member's access to EPHI and other sources of protected health information (PHI) including access to rooms or facilities where PHI is located will be terminated or suspended in these circumstances:

1. 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

2. If the workforce member or management has reason to believe the user's password has been compromised

3. If the workforce member resigns, is terminated, suspended, retires, or is away on unapproved leave

4. If the workforce member's including business associate's work role changes and systems access is no longer justified

If the workforce member is on leave of absence and the user's system access will not be required for more than three weeks, management shall suspend the user's account until the workforce member returns from their leave of absence.

Modifications of Access
If a workforce member transfers to another program or changes their work role within the same program, the workforce member's new/manager or supervisor is responsible for the evaluating the member's current access and for requesting new access to EPHI commensurate with the workforce member's new work role and responsibilities.

Ongoing Compliance for Access
In order to ensure that workforce members only have access to EPHI when it is required for their job function, the following actions shall be implemented:

1. Every new user ID or logon account that has not been used after 30 consecutive calendar days since creation shall be investigated to determine if the workforce member still requires access to EPHI.

2. At least annually, Information Systems staff shall send managers or designees a list of assigned workforce members for the Avatar application.

3. At least annually the Information Systems staff shall send managers or deigned:

    a. A list of workforce members and their access to shared folders containing EPHI.

    b. A list of workforce members approved for access to Virtual Private Network (VPN)

4. The managers or their designees shall them notify Information Systems staff of any workforce member who no longer requires access.

4. Policy Responsibilities

Managers or Designee Responsibilities

1. Request access for new employees.

2. Ensure the access to EPHI granted to each of their workforce members us the minimum necessary access required for workforce member's work role and responsibilities.

3. Request termination of access if the workforce member no longer requires access (i.e., resignation or change of classification, etc.).

4. Notify Information Systems staff immediately if a workforce member is being suspended, or terminated with cause.

5. Validate new Users IDs or logon accounts that are not used within 30 days of creation via the report generated by IS.

6. Review annual folder access reports and VPN access reports prepared by IS staff and verity if the workforce members still require access to the EPHI.

7. Follow the appropriate security procedures when granting emergency access.

Information Systems Responsibilities

1. Ensure members of the workforce have signed the Initial Security Awareness Training form and are properly trained before providing access to EPHI.

2. At least annually, Information Systems staff shall managers or designees a list of all workforce members for send the Avatar application.

3. When required, provide management with the appropriate support for granting emergency access.

4. Immediately, upon written notification from a manager or Human Resources, remove or modify a workforce member's access to EPHI.

5. Notify manager/designee when a user ID or logon account has not been used within 30 days.

6. At least annually months provide managers or designee:

   a. A list of workforce members and their access to shared folders containing EPHI.

   b. A list of workforce members approved for access to Virtual Private Network (VPN).

Workforce Members Responsibilities

Each user of a system or application that contains EPHI shall:

1. Read and sign the Initial Security Awareness Training form and the Electronic Signature form,

2. Follow all County and departmental policies and requirements

3. Complete a HIPAA Privacy and Security training

4. Immediately report all security incidents to their supervisor.

Related Policies and Regulations

Policies:

1. 01-128 HIPAA – Audit Controls

Regulations:

1. 45 C.R.R. Section 164.308 (a)(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)(3)(ii)(C): Termination procedures (Addressable) Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends of as required by determinations made as specified in paragraph (a)(3)(i)(B) of this section.

4. 45 C.F.R. Section 164.308 (a)(4)(i): Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

5. 45 C.F.R. Section 164.308 (a)(4)(ii)(B): Access authorization(Addressable). Implement policies and procedures for granting access to electronic protected health information,

for example through access to a workstation, transaction, program, process, of other mechanism.

6. 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.

7. 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 of software programs that have been granted access rights as specified in Section 164.308(a)(4).

8. 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.