


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

<b>SUBJECT:</b> HIPAA - Information System Monitoring	<b>POLICY NO:</b> 01-296
<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 5
	<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:** The purpose of this policy is to ensure that unauthorized access and usage of information systems will be detected, reported and acted upon by recording and periodically examining activity within information systems that contain or use electronic protected health information.

**NOTES:** ICBHS is responsible for the safety and security of data on its network, the electronic health record and the equipment used to support the ICBHS network infrastructure.

ICBHS shall ensure that all devices are configured to allow logging and recording of required security parameters. These logging parameters are specified in the standards section of this policy.

Monitoring goals include the following:

- Tracking both successful and unsuccessful attempts to access the electronic health record, IT devices, services and applications
- Auditing access and changes to PHI in the Electronic Health Record (EHR) applications
- Reviewing changes to rights of any user
- Evaluating all uses of administrative rights

- Tracking installation of new software or software components (e.g. drivers)
- Detecting misuse of protocols, components or connections

The primary tool for monitoring shall be the various audit logs that are maintained in the electronic health record, servers, workstations and other devices. These must be configured to collect and store the logged parameters. Critical system logs should be periodically inspected by assigned information technology staff. Other logs should be available to assist incident management.

The County of Imperial Information & Technical Services (ITS) is responsible for the installation of new technology infrastructure, ensuring operation of existing resources, and maintaining ICBHS and county network infrastructure.

The Information Systems BHM is responsible for administering the information security functions within ICBHS and managing the maintenance of information technology security resources within ICBHS.

The Systems Technology Analyst from ITS is responsible for implementing monitoring tools on ICBHS information technology infrastructure. Systems Technology Analyst is also responsible for ensuring Systems Technology Technicians perform corrective action for problems submitted by staff through the helpdesk.

**DEFINITIONS:** None

**POLICY OWNER:** Security Officer

**POLICY:** All ICBHS computers and network activity are subject to ongoing and unannounced monitoring and security audits by County ITS and as deemed necessary by executive management personnel. The inappropriate use of the systems and or/ networks which violate ICBHS and County of Imperial Information Systems department polices, local, state and ICBHS electronic health record, computers and network activity are subject to ongoing and unannounced monitoring and security audits by Information Systems and Systems Technology staff and as deemed necessary by management. The

inappropriate use of the systems and or/ networks which violate ICBHS and ITS department policies, local, state and federal laws and will be investigated with appropriate notification to authorities.

Automated tools and applications will be used to provide real time notification of detected wrongdoing and vulnerability exploitation.

The automated tools and applications will be administered to monitor the following:

- A. Successful user login
- B. Unsuccessful user login
- C. Changes to access rights
- D. Changes to data ownership
- E. Changes to system security policy
- F. Changes to the system clock
- G. Installation of new software
- H. Firewall logs
- I. User account access logs
- J. Network scanning logs
- K. System error logs
- L. Application logs
- M. Data backup and recovery logs

To ensure the security and protection of protected health information and data within the ICBHS technology infrastructure the following checks will be performed periodically on ICBHS network and the equipment used.

- A. Unauthorized network devices
- B. Unsecured sharing of devices
- C. Unauthorized personal web services
- D. Operating System and Software Licenses
- E. Appropriate help desk ticket submissions for removal, transfer, or installation of technology equipment.

Additionally automated tools must be formatted according the following:

- A. All logged event entries must be date and time stamped

and identify the user account used.

- B. All logs should be sized to hold at least one week's log entries.
- C. All user access to PHI must be logged by the application and the logs retained for a minimum of 6 years.
- D. Event logs must not be deactivated or modified without specific approval from the Information Systems BHM.
- E. Event logs should only be accessed by authorized administrators for review purposes and any such access must be logged. Wherever possible, utilize automated exception processing to identify log review areas.
- F. User access logs for all applications that display, process, store or transmit PHI should be reviewed at least once each month.
  - a. A system log review plan should be developed and updated periodically based on known and potential risk and vulnerability areas.
  - b. The Security Compliance Officer should sign-off that the logs have been reviewed and exceptions followed up on.
- G. Any unusual or suspicious access or changes must be reported to the Security Compliance Officer and Information Systems BHM immediately upon discovery.

### **Related Policies and Regulations**

Policies:

Regulations:

1. HIPAA Standard 45 .C.F.R. § 164.312 (b): Audit controls.  
*Implement hardware, software, and/or procedural mechanisms that*

*record and examine activity in information systems that contain or use electronic protected health information.*

2. HIPAA Standard 45 C.F.R. § 164.308 (a)(1)(i): Security management process. *Implement policies and procedures to prevent, detect, contain, and correct security violations*
  - HIPAA Implementation Specification 45 C.F.R. § 164.308 (a)(1)(ii)(D): Information system activity review (Required). *Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*
3. HIPAA Standard 45 C.F.R. § 164.308 (a)(5)(i): Standard: Security awareness and training. *Implement a security awareness and training program for all members of its workforce (including management).*
  - HIPAA Implementation Specification 45 C.F.R. § 164.308 (a)(5)(ii)(C): Implement Log-in monitoring (Addressable). *Procedures for monitoring log-in attempts and reporting discrepancies.*
4. HIPAA 45 CFR § 164.528