


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

POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA - Risk Management	POLICY NO: 01-289
SECTION: Administration	EFFECTIVE DATE: 6-8-16
REFERENCE: 45 C.F.R. Subtitle A, Subchapter C, Part 164	PAGE: 1 of 3
	SUPERSEDES: New Policy
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	APPROVED BY: 

PURPOSE: The purpose of this policy is to establish a risk management framework, methodology and procedures that will reduce the level of privacy and security risks ICBHS faces to a reasonable and appropriate level, and meets the requirements of the HIPAA Security Rule.

NOTES: None

DEFINITIONS: **HIPAA HITECH Express:** is a web-based solution that provides guidance through the privacy and security compliance process.

POLICY OWNER: Security Officer

POLICY: A Risk Management Plan is prepared, based on industry-wide threat and risk profiles, to guide the implementation of critical risk abatement and security management functions as needed. The fundamental privacy and security procedures are established to manage the initial risk remediation and are continued in an ongoing program of risk assessment, analysis and remediation. Once initial remediation tasks and a scan of the enterprise for vulnerabilities have been completed, a follow-up risk analysis will be conducted.

This policy mandates the creation and implementation of a Risk

Management Plan. This document provides the roles, tasks and ongoing maintenance and monitoring requirements of the organization's Risk Management Program, including the implementation of the Risk Management Plan.

Key aspects of the Risk Management Plan are:

- Documented threats to the confidentiality, integrity and availability of ICBHS data and business process
- Identified vulnerabilities in the implementation of administrative, operational and technical controls at ICBHS
- Development and maintenance of the inventory of PHI and all resources, devices and applications that create, process, store or transmit it
- Selection of reasonable and appropriate controls to protect PHI in all phases of its lifecycle, during storage, transmission and in emergency situations
- Implementation of the controls
- Assessment of the effectiveness of the controls
- A schedule of maintenance and monitoring activities as required by controls

The Risk Management Plan and all required implementation, monitoring and assessment artifacts are archived in the HIPAA HITECH EXPRESS Security Documentation Library as described in Policy 01-290, Security Management.

STANDARDS:

The following actions must be accomplished:

1. Development of a Risk Management Plan based on a risk assessment that is reviewed and revised annually.
2. An up-to-date inventory of all resources that create, receive, maintain or transmit protected health information.
3. A risk assessment that incorporates threats,

vulnerabilities and potential impacts to the organization, and provides a roadmap for a risk mitigation work plan to mitigate unacceptable risks, based on the relative risk of identified administrative, technical and physical vulnerabilities to the organization.

4. A set of privacy and security controls with associated baseline configurations that are documented, implemented and monitored.
5. Documentation of all elements required by the Risk Management Plan in the HIPAA HITECH EXPRESS Security Documentation Library.
6. Annual review of all Privacy and Security Policies and Standard Operating Procedures.

Related Policies and Regulations

Policies:

1. 01-290 HIPAA - Security Management Policy

Regulations:

1. 45 C.F.R. § 164.308 (a)(1)(i): Standard: Security management process. Implement policies and procedures to prevent, detect, contain and correct security violations.
2. 45 C.F.R. § 164.308 (a)(1)(ii)(B): Risk management (Required). Implement necessary security measures to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).
3. 45 C.F.R. § 164.308 (a)(1)(ii)(A): Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity.