


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

POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA - Security Management	POLICY NO: 01-290
SECTION: Administration	EFFECTIVE DATE: 6-8-16
REFERENCE: 45 C.F.R. Subtitle A, Subchapter C, Part 164	PAGE: 1 of 8
	SUPERSEDES: New Policy
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	APPROVED BY: 

PURPOSE: To provide guidelines for the governance of IT Security at ICBHS.

NOTES: This security management structure includes an interconnected set of policies, plans, procedures, documentation, and role assignments. The end result for the organization is a secure, compliant and auditable environment. This policy also mandates a series of additional policies, plans, procedures, documentation and roles that govern all security activities at ICBHS.

DEFINITIONS:

POLICY OWNER: Security Officer

POLICY: The Security and Privacy Officer(s) in conjunction with management shall create, document, and implement policies and procedures that maintain compliance with the HIPAA Privacy and Security rules, as amended by any subsequent Federal, State or Local legislative or regulatory actions, through an ongoing Privacy and Security Risk Management Program as outlined in the Policy 01-289, Risk Management. This policy is the umbrella policy that describes the set of policies that

govern all aspects of privacy and IT security compliance at ICBHS. An online HIPAA High Tech Express Security Document Library will be used to store all documentation required for the implementation and execution of the enterprise security program. The security program will consist of the following components:

1. Policies

Policies define how the organization will address specific security areas. The Director of ICBHS or designee approves policies. All policies that are in effect are binding on the entire staff of ICBHS and may be binding on guests, visitors, contractors or business associates. A Policy Checklist will be maintained of all policies that are included in the Policy and Procedure manuals. Policies consist of a:

- o Purpose Statement
- o Policy Statement
- o Policy Owner
- o Policy Standards
- o Related Policy or Standard Operating Procedures Reference
- o HIPAA Security Rule Cross Reference

2. Plans

There are certain plans identified in the Policy Checklist that are required for compliance and other business reasons that must be developed, adopted, implemented and maintained. These plans combine procedures with schedules, documentation and assignments to prepare for various security and privacy contingencies and activities.

3. Corrective Actions

Plans of Action and Milestones (POA&M) are the mechanism by which the organization shows progress at resolving vulnerabilities, closing gaps and decreasing risk. For extensive or difficult projects there should be sufficient detail in the milestones to show intermediate progress.

4. Procedures

Procedures are identified in the Policy Checklist. They are the detail specifications for activities undertaken to implement the policies and plans. Procedures document the tasks that must be completed, the schedule for completion of these tasks, oversight responsibility for the procedure and the documentation requirements.

5. Documentation

A Security Document Library will be created to hold and store all security documentation including, but not limited to, all the policies, plans, procedures, implementation documentation, inventory of equipment and software, inventory of PHI, business associate agreements and risk management decisions. This document library shall retain a history of all documents for a period of 6 years.

6. Role Assignments

Certain roles and responsibilities are defined in ICBHS policies, plans and procedures. These are used to assign responsibility and accountability for the tasks and outcomes of security activities. The roles and the assignment of individuals to each role shall be documented and regularly updated as changes occur. Roles are different than official positions in the organization. A role is a job function that is assigned to one or more people and an individual may be responsible for one or more roles. Refer to the HIPAA Privacy and Security Roles Policy (01-77) for more information on these roles.

STANDARDS:

1. Policies

- Policies will have an owner who is responsible for the development, approval, implementation, execution and maintenance of each policy.

- The ICBHS Director or designee will approve new and updated policies.
- All policies should be reviewed and updated at least annually based on organization and regulatory changes.
- The list of ICBHS policies is found in the Policy Checklist maintained in the Security Document Library at the *HIPAA HITECH EXPRESS* online application.

2. Plans

- The development of Plans is generally a task requirement needed to fully implement specific policies. The policy owner is responsible for the development, approval, implementation, execution and maintenance of plans needed to implement those policies.
- The ICBHS Director or designee will approve new and updated plans.
- Each Plan should be reviewed annually or as needed to adapt to changes in the work environment, or to address security incidents or training issues.
- The list of ICBHS policies is found in the Policy Checklist maintained in the Security Document Library at the *HIPAA HITECH EXPRESS* online application.

3. Plans of Action and Milestones (POA&M)

- The Security Officer shall create and maintain a set of Plans of Action and Milestones (POA&Ms) that address unacceptable risks, vulnerabilities and compliance gaps that must be remediated.
- POA&Ms must be documented with the following information:
 - Start date
 - Scheduled completion date
 - Owner of the project (aka the responsible party)
 - Actual completion date
- POA&Ms are managed using the work plan in the *HIPAA HITECH EXPRESS* online application.

4. Documentation

- All policies, plans, procedures, assessments and the evidence of complete and correct implementation are to be stored in the online Security Document Library.
- The contents of the Security Document Library should be audited at least once each year.
- Inventories of PHI interfaces and applications, devices and media that create, store or transmit PHI, and Business Associate Agreements shall be reviewed and updated at least once each year.
- Documents shall be retained in the Security Document Library at the *HIPAA HITECH EXPRESS* online application for a minimum of 6 years.

5. Roles and Responsibilities

- Each document (policy, plan or procedure) shall have a designated owner with responsibility and accountability to ensure that it is implemented and the necessary approval is documented.
- The list of roles, including those assigned to the role, shall be documented in the Security Document Library.
- The Security Compliance Officer at ICBHS is responsible for overall management of security. Where necessary or expedient, the Security Compliance Officer can delegate responsibility for policies, plans, procedures and documentation to others as defined in the Security Roles Policy.

Related Policies and Regulations:

Policies:

1. 01-77 HIPAA - Privacy and Security Roles
2. 01-289 HIPAA - Risk Management Policy

Regulations:

1. § 164.306 Security standards: General rules.

- (a) General requirements. Covered entities must do the following:
 - (a)(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
 - (a)(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
 - (a)(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
 - (a)(4) Ensure compliance with this subpart by its workforce.
- (b) Flexibility of approach.
 - (b)(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
 - (b)(2) In deciding which security measures to use, a covered entity must take into account the following factors:
 - (i) The size, complexity, and capabilities of the covered entity.
 - (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
 - (iii) The costs of security measures.
 - (iv) The probability and criticality of potential risks to electronic protected health information.
- (c) Standards. A covered entity must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.
- (d) Implementation specifications. In this subpart:
 - (d)(1) Implementation specifications are required

or addressable. If an implementation specification is required, the word ``Required'' appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word ``Addressable'' appears in parentheses after the title of the implementation specification.

(d)(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications. (1) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must-

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and

(ii) As applicable to the entity-

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate-

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) Maintenance. Security measures implemented to comply with standards and implementation specifications adopted under § 164.105. This subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.

2. HIPAA Security Rule 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.
3. HIPAA Security Rule 45 C.F.R. § 164.316 **Policies and procedures and documentation requirements**. A covered entity must, in accordance with § 164.306:
- (a) Standard: **Policies and procedures**. Implement comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
 - (b)(1) Standard: **Documentation**.
 - (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and
 - (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
 - (b)(2) Implementation specifications:
 - (i) **Time limit** (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
 - (ii) **Availability** (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
 - (iii) **Updates** (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.