


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

POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA - Security Incident Reporting and Response	POLICY NO: 01-237
SECTION: Administration	EFFECTIVE DATE: 9-17-21
REFERENCE: 45 C.F.R. Section 164.308(a)(6)(i), 164.308(a)(7)(i)	PAGE: 1 of 7
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	SUPERSEDES: 10-14-15
	APPROVED BY: 

PURPOSE: To define ICBHS' incident response policy and process. This includes identification and response to suspected or known security incidents, the mitigation of the harmful effects of known or suspected security incidents to the extent possible, and the documentation of security incidents and their outcomes.

NOTES: The objectives of the incident response plan include:

- Timely detection and reporting of a security incident
- Containing the impact of the incident
- Recovering quickly from the incident
- Determining how the incident occurred
- Implementing mitigation step to reduce the risk of future incidents
- Communication effectively to the organization about the incident
- Ensuring involvement of critical stakeholders in response activities

- Documenting the incident and updating the response plan

DEFINITIONS:

Availability: is defined in the Security Rule, at Section 164.304 as "the property that data or information is accessible and useable upon demand by an authorized user".

Confidentiality: is defined in the Security Rule, at Section 164.304 as "the property that data or information is not made available or disclosed to unauthorized persons or processes.

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

ICBHS: Imperial County Behavioral Health Services.

Integrity: is defined in the Security Rule, at Section 164.304 as "the property that data or information have not been altered or destroyed in an unauthorized manner."

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.

IS: Information Systems.

Security Incident is defined as, "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an 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". For the purposes of this policy, workforce members also includes those assigned to Imperial County Information Technology and Systems (ITS).

POLICY OWNER: Security Officer

POLICY: ICBHS shall identify, document, respond to, and remediate unauthorized use of the systems that contain EPHI. ICBHS' ability to successfully respond to potential security incidents is dependent of timely detection and notification of security events through people, processes, and technologies. All members of the workforce and contractors will be provided training on identifying and reporting security incidents.

For every event it is important that the event be analyzed in a consistent and timely manner. As part of the analysis process, severity classification levels will be assigned to all verified incidents so that the appropriate response and escalation procedure can be determined.

Some regulations around incident responses also require timely notification of regulatory bodies.

1. **Incident Reporting**

All incident reporting, threats to, or violations of, the confidentiality, integrity or availability of EPHI shall be reported and responded to promptly. Incidents that shall be reported include, but are not limited to:

- a. EPHI data loss due to disaster, failure, error, theft
- b. Loss of any electronic media that contains EPHI
- c. Loss of integrity or EPHI
- d. Virus, worm, or other malicious code attacks that interfere with the operation of information systems with EPHI

- e. Persistent network or system intrusion attempts from a particular entity
- f. Unauthorized access to EPHI, as EPHI based system of network
- g. Facility incidents, including but not limited to:
 - Unauthorized person found in HIPAA covered entity's facility
 - Facility break-in leading to the theft of media with EPHI
 - Lost or stolen physical key
- h. Inappropriately obtained passwords that are used to access EPHI
- i. Corrupted backup tapes that do not allow restoration of EPHI
- j. Failure to terminate the account of a former employee that is then used by an unauthorized user to access information systems with EPHI
- k. Providing media with EPHI, such as a PC hard drive or laptop, to another user who is not authorized to access the EPHI prior to removing the stored EPHI

2. **Detection and Reporting**

Workforce members shall notify their manager or supervisor of any suspected or confirmed security incident. The manager or supervisor shall report the incident to the IS manager/designee and submit a Security Incident Alert Form (Appendix A). The following information should be provided:

- a. Name or caller
- b. Program/Unit
- c. Office/cell number
- d. Time of security event discovery
- e. Location of discovery
- f. Description of event

3. Incident Analysis and Response

The IS Manager/designee shall receive and record basic information on the incident and forward the information to the appropriate staff for response to that type of incident, i.e. a computer virus incident reported to the County ITS staff who provides anti-virus support.

The County ITS staff receiving the security incident service request shall perform their assigned responsibilities to respond to and/or mitigate any incident consequences. The IS manager/designee is responsible for determining if a possible EPHI breach has resulted from the incident and shall notify the Security Officer.

The ICBHS Security Officer shall evaluate the incident to determine if a breach of EPHI occurred based on past history and the typical security incidents listed above. If it is determined that a breach has occurred, the Security Officer will complete a Security Incident Report form (Appendix B) and perform any mandated notifications according to Policy 01-158.

4. Containment

A Containment Plan will be developed to minimize further damage to the organization. The Containment Plan will include the following activities:

- Identify and mitigate vulnerabilities suspected to have been exploited.
- Based on the severity of incident and criticality of systems involved, invoke the ICBHS' Business Continuity Plan.

5. Remediation and Recovery

A Remediation Plan defines the steps required to recover the affected business operations of data. The Remediation Plan includes the following activities:

- Determine any evidence that needs to be maintained for forensic and audit purposes.
- Determine if systems, data, and/or hardware needs to be restored or rebuilt.
- A corrective and preventive action plan shall be developed.
- Update and modify any policies, procedures, and training to reduce the risk of a similar incident.

6. **Incident Logging**

All HIPAA Security incidents and their outcomes will be logged and documented by the IS Manger/designee on the Security Incident Form (Appendix C).

Each fiscal quarter, the IS Manager/designee shall provide the ICBHS Security Officer with a record of all incidents logged. The Security officer shall retain these incident reports for six years.

7. **Policy Responsibilities:**

1. Workforce Member Responsibilities

- Workforce members are responsible to promptly report any potential security related incidents to their manager or supervisor, or directly to the IS Manager/designee.

2. Supervisor or Manager Responsibilities

- Ensure that the IS Manager/designee and the Security Officer are notified of the event.

3. IS Manager Responsibilities

- Ensure that facility-related security incidents are reported and responded to promptly.

Related Policies and Regulations:

Policies: 01-232 HIPAA- PHI Protection Policy

Regulations:

1. 45 C.F.R. Section 164.308(a)(6)(i): Standard: Security Incident Procedures> Implement policies and procedures to address security incidents. (ii) Implementation Specifications: Response and Reporting (Required). Identify and respond to suspected known security incidents; mitigate, to the extent practicable, harmful effects or security incidents that are known to the covered entity; and document security incidents and their outcomes.
2. 45 C.F.R. Section 164.308(a)(7)(i): Standard Contingency Plan. Establish and implement as needed policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, natural disaster) that damages systems that contain electronic protected health information.