


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

**POLICY AND PROCEDURE MANUAL**

<b>SUBJECT:</b> HIPAA - Security Incident Notification and Mandatory Reporting	<b>POLICY NO:</b> 01-158
	<b>EFFECTIVE DATE:</b> 9-17-21
<b>SECTION:</b> Administration	<b>PAGE:</b> 1 of 11
	<b>SUPERSEDES:</b> 6-8-16
<b>REFERENCE:</b> DHCS Mental Health Plan Contract, Exhibit F DHCS Intergovernmental Agreement, Exhibit F	<b>APPROVED BY:</b> 
<b>AUTHORITY:</b> Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	

**PURPOSE:** To establish a policy for the prompt reporting of any breach or security incident to the State Department of Health Care Services upon the discovery of a breach of unsecured ICBHS patient PII, PI, or PHI in electronic media or in any other media if the PII, PI, or PHI was, or is reasonably believed to have been, accessed or acquired by an authorized person.

**DEFINITIONS:**

**CIPA:** The California Information Practices Act of 1977.

**DHCS:** State Department of Health Care Services.

**Discovery:** A breach shall be treated as discovered as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or agent of ICBHS.

**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.

**IEA:** Information Exchange Agreement currently in effect between the Social Security Administration (SSAA) and the California Health and Human Services.

**Personal Identifiable Information (PII):** Any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mothers's maiden name, etc.,

**Personal Information (PI):** Any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. Civil Code § 1798.3(a)

**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.

**Security Incident:** Means the attempted or successful

unauthorized access, use, disclosure, modification, or destruction of PHI, or confidential data utilized in complying with ICBHS contract(s) with DHCS; or interference with system operations in an information system that processes, maintains or stores PHI.

**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.

**POLICY:** All members of the ICBHS workforce have the duty to immediately report any unauthorized use of systems that contain EPHI according to Policy 01-237, HIPAA - Security Incident Reporting and Response. The ICBHS Security Officer or designee shall evaluate the incident to determine if a breach of EPHI occurred. If it is determined that a breach has occurred, the ICBHS Security Officer or designee shall notify DHCS, immediately by telephone call plus email or fax, upon the discovery of a breach of unsecured PII, PI, or PHI in electronic media or in any other media if the PII, PI, or PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.

The ICBHS Security Officer or designee shall notify DHCS within 24 hours by email or fax of the discovery of any suspected security incident, intrusion, or unauthorized access, use or disclosure of PHI in violation of ICBHS' agreement(s) with DHCS.

The ICBHS Security Officer or designee shall notify the DHCS Program Contract Manager and the DHCS Information Security Officer. If the incident occurs after business

hours or on a weekend or holiday and involves electronic PII, PI, or PHI notice shall be provided by calling the DHCS Information Security Officer. Notice shall be made by using the DHCS "Privacy Incident Report" form, including all of the information known at the time. The

DHCS Information Security Officer's contact information is:

Information Security Officer  
Email: iso@dhcs.ca.gov  
Telephone: ITSD Service Desk (916) 440-7000

ICBHS shall take prompt corrective action to cure any risks or damages involved in the breach and to protect the operating environment and any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

The ICBHS Security Officer or designee shall investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PII, PI, or PHI. Within 72 hours of the discovery, ICBHS will submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form.

Within 10 working days of the discovery of the breach or unauthorized use or disclosure, the ICBHS Security Officer or designee will provide a complete report of the investigation to the DHCS Program Contract Manager and the DHCS Information Security Officer. The report shall be submitted in the "Privacy Incident Report" form and shall include:

- An assessment if all known factors relevant to a determination of whether a breach occurred
- A full, detailed corrective action plan, including information on measures that were taken to halt or contain the improper use or disclosure

If DHCS needs additional information, ICBHS will make

reasonable efforts to provide DHCS the information. If ICBHS needs more than 10 days from the discovery to submit a complete report, ICBHS will request an extension from DHCS, in which case ICBHS will sent periodic updates until a complete report is submitted.

If necessary, a Supplemental Report may be used to submit revised or additional information after the complete report is submitted, by submitting the revised or

additional information on an updated "Privacy Incident Report" form.

DHCS will review and approve the determination of whether a breach occurred and individual notification are required and the corrective action plan.

If the case of a breach of DHCS PII, PI, or PHI is attributable to ICBHS or its agents, subcontractors or vendors, ICBHS is responsible for all required reporting of the breach as specified in CIPA § 1798.29(a)-(d) and may be required under the IEA. ICBHS will bear the cost of required notification to individuals as well as any costs associated with the breach. The DHCS Program Contract Manager and the DHCS Information Security Officer shall approve the time, manner and content of any such notification and there review and approval must be obtained before the notification are made. If ICBHS has reason to believe that duplicate reporting of the breach or incident may occur because its subcontractors, agents, vendors may report the breach or incident to DHCS in addition to ICBHS, ICBHS shall notify DHCS, and DHCS and ICBHS will take appropriate action to prevent duplicate reporting.

In the event DHCS determines a breach occurred and individual notification is required, the ICBHS Security Officer or designee shall report the determination to the ICBHS Privacy Officer or designee. The ICBHS Privacy Officer is responsible for all breach notification processes to the appropriate entities:

**Timeliness of Notification:** Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of the breach by ICBHS or a business associate involved. It is the responsibility of ICBHS to demonstrate that all notifications were made as required.

**Law Enforcement Exception:** If law enforcement asks ICBHS to delay notification/reporting because it would impede a criminal investigation or cause damage to national security, then ICBHS will delay notification/reporting until the investigation is completed. If the request is made orally, ICBHS will document the statement, identify the law enforcement agency or official making the statement, and temporarily refrain from notification or reporting, but no

longer than 30 days, unless a written statement is submitted during that time.

**Content of the Notice:** The notice shall be written in plain language and must contain the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured protected health information that were involved in the breach (e.g. full name, Social Security number, date of birth, home address, account number, diagnoses, disability code, or other types of information).
- Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- A brief description of what ICBHS is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

- Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an email address, or postal address.

**Methods of Notification:** The method of notification will depend on the individuals/entities to be notified.

**Notification of Individual(s):** Notice shall be provided promptly and in the following form:

- Written notification by first class mail to the individual at the last known address of the individual, unless the individual has specified a preference for email or other means and such agreement has not been withdrawn.
- If ICBHS knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification shall be made by first class mail to the next of kin or personal representative.
- If the individual affected is a minor, the notice will be sent to the parent/guardian/caregiver.
- If notification is urgent because of possible imminent misuse of the unsecured PHI, ICBHS will notify individuals by phone or other means as is appropriate; additionally, written notification is also required.

**Breach involving less than ten (10) individuals who cannot be reached:** If the contact information for less than 10 individuals is outdated or insufficient, substitute notice may be provided by telephone, posting on a website, or other written notice.

**Breach involving more than ten (10) individuals who cannot be reached:** If the contact information for more than 10 individuals is outdated or insufficient, substitute notices must be provided through:

- Conspicuous posting for 90 days on the home page of the website.
- Conspicuous notice in major print or broadcast media in geographic areas where individuals affected by the breach likely reside.

Either method requires a minimum posting of 90 days and a toll free number where an individual can call to find out if his or her unsecured PHI or PII was included in the breach.

**Breach involving five hundred (500) individuals or more:** If the breach affects more than 500 individuals, ICBHS must provide notice to:

- Prominent media outlets serving that state
- Each affected individual
- Secretary of Health and Human Services

**Mandatory Reporting to DHHS:** The Secretary of the DHHS must be notified of all breaches. In situations where 500 or more individuals are involved in a single breach, the notice must be provided immediately. If fewer than 500 individuals are involved, ICBHS may maintain a breach log or other documentation which must be submitted to the DHHS.

A form has been developed that may be complete online that is titled Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information. It can be found at [www.dhhs.gov](http://www.dhhs.gov).

**Maintenance of Breach Log:** The ICBHS Privacy Officer shall maintain a process to log all breaches of unsecured PHI regardless of the number of individuals affected. The following information should be logged for each breach:

- A description of what happened, including the date of the breach, the date of discovery, and the number of individuals affected, if known.



- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
- A description of the action taken with regard to notification of individuals regarding the breach.
- Resolution steps taken to mitigate harm to the individuals, and to protect against further breaches.

**Breaches by Business Associates:** Upon discovery of a breach of unsecured PHI, a business associate must immediately notify the ICBHS Privacy Officer. Notification may be delayed if so advised by a law enforcement official pursuant to 45 CFR § 164.412.

A business associate's notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.

Notice to ICBHS must include, to the extent possible:

- The identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been accessed, used, or disclosed during the breach.
- Any other information that ICBHS is required to include in the notification to the individual under 45 CFR § 164.404(c) at the time the business associate is required to notify ICBHS or promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period defined in 45 CFR § 164.410 (b) has elapsed, including:
  1. A brief description of what happened, including the date of the breach and the date of discovery

of the breach, if known;

2. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved;
3. Any steps the individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what the business associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against any future breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web site, or postal address.

A business associate shall provide ICBHS all specific and pertinent information about the breach, including the information listed in 1-5 above, if not provided, to permit ICBHS to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after the business associate's initial report of the breach to the ICBHS Privacy Officer.

A business associate shall continue to provide all additional pertinent information about the breach to ICBHS as it may become available, reporting in increments of five (5) business days after the last report to ICBHS. A business associate shall respond in good faith to any reasonable requests for further information, or follow-up information after report to ICBHS, when requested.

ICBHS may require a business associate to provide notices to the individuals as required under 45 CFR § 164.404, if it is reasonable to do so under the circumstances, at the

sole discretion of ICBHS.

In the event that the business associate is responsible for a breach of unsecured PHI in violation of the HIPAA Privacy Rule, the business associate will have the burden of demonstrating that it made all notifications to ICBHS consistent with this policy and as required by the breach notification regulations, or in the alternative, that the acquisition, access, use, or disclosure did not constitute a breach.

A business associate shall maintain documentation of all required notification of a breach or its risk assessment under 45 CFR § 164.402 to demonstrate that a breach did not occur.

A business associate shall bear all expenses or other costs associated with the breach and shall reimburse ICBHS for all expenses ICBHS incurs in addressing the breach and consequences thereof, including cost of investigation, notification, remediation, documentation or other costs associated with addressing the breach.