


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

SUBJECT: HIPAA - Breach Notification And Mandatory Reporting	POLICY NO: 01-191
SECTION: Administration	EFFECTIVE DATE: 9-17-21
REFERENCE: 45 C.F.R. Subtitle A, Subchapter C, Parts 160 and 164	PAGE: 1 of 11
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	SUPERSEDES: 6-8-16
	APPROVED BY: 

PURPOSE: To provide guidance for breach notification when impermissible or unauthorized access, acquisition, use and/or disclosure of ICBHS' patient protected health information occurs.

NOTES: Final breach notification regulations, effective for breaches discovered on or after September 23, 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act and finalized by the Omnibus Bill, effective March 23, 2013, by requiring HIPAA covered components and their business associates to provide notification following a breach of **unsecured** protected health information.

The regulations, developed by the Office for Civil Rights require HIPAA covered components to promptly notify affected individuals of a breach of their protected health information, as well as the Health and Human Services (HHS) Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered components to notify the covered

component.

DEFINITIONS:

Access: means the ability of the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Breach: means the unauthorized access or acquisition of data that compromises the security, confidentiality or integrity of personally identifiable information (PII) and protected health information (PHI) Data may be in electronic or hardcopy and may consist of a single piece of data and/or an entire data system.

Examples of a "breach" include, but are not limited to:

- Faxing of a PII or PHI to the wrong number outside the facility.
- A stolen laptop computer or other electronic device (i.e., flashdrive) containing unencrypted individually identifiable information.
- An employee searching data systems with PII or PHI without a legitimate business to access the information.
- Leaving individually identifiable information in a public place.
- Accessing electronic health records for information on family, co-workers, or friends, or neighbor out of curiosity, or without a business related purpose.
- Briefcase containing client information stolen from car.
- Medical record copies lost in the mailing process and never received.
- Misfiled information in another client's chart which is brought to ICBHS' attention by the client.

Exceptions: the term "breach does not include:

- Unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of ICBHS if the acquisition, access, or use was made in good faith and within the course and scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.

Example: A staff member accessed the wrong medical record, but when he/she realized the error, the staff member closed the record and did not retain any information.

- Any inadvertent disclosure by a person who is authorized to access PHI at ICBHS to another person authorized to access PHI at ICBHS and the information is not further used or disclosed in a manner not permitted by the Privacy Rule.

Example: PHI of a Physician A is disclosed to a nurse who works with Physician B. The nurse does not use or further disclose the information and reports the error.

- A disclosure of PHI where ICBHS has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Example: sending PHI in the mail to the wrong address where the mail is returned unopened to the post office as undeliverable, or where the nurse mistakenly hands discharge papers to the wrong client, quickly realized the mistake, and recovers the PHI before the client has time to read it.

Discovery of breach: a breach is treated discovered on the first day that the breach is known or when by exercising reasonable diligence, the breach would have been known (includes breaches by the organization's business associates.

ICBHS: Imperial County Behavioral Health Services.

Individually Identifiable: means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the

individual, such as the client's name, address, electronic email address, telephone number, social security number, or other information that alone or in combination with other publicly available information, reveals the individual's identity.

Protected Health information (PHI): Protected Health information means individually identifiable information that is: transmitted by electronic media, maintained in electronic media; or transmitted or maintained in any other form or medium.

Unauthorized Access: means the inappropriate review or viewing without the direct need for diagnosis, treatment, or other lawful use permitted by the confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of division 1 of the Civil Code) or by other statutes or regulations governing the lawful access, use, or disclosure of medical information. (CA Health and Safety Code, Section 130201 (e)).

Unsecured Protected Health Information: Protected health information (PHI) that is not rendered unusable, unreadable, or undecipherable to unauthorized individuals through the use of technology or methodology specified in federal guidance documents (HITACH, Section 13402 (h)).

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 to the ICBHS Privacy Officer or designee any acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rules which compromises the security or privacy of PHI.

ICBHS Workforce Detection and Reporting Requirements:

ICBHS workforce members shall report any potential incident unlawful or unauthorized access of unsecured PHI to their

supervisor as soon as it is discovered. A breach is to be treated as "discovered" as of the first day on which such breach is known to ICBHS, or, by exercising reasonable diligence would have been known to ICBHS.

ICBHS shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, or any person, other than the person committing the breach, who is a workforce member or agent (business associate) of ICBHS. A manager/supervisor who is notified of a potential breach shall immediately notify the ICBHS Privacy Officer or designee via telephone. If the manager/supervisor is unable to make contact with the ICBHS Privacy Officer or designee via telephone, email notification may be provided. The manager/supervisor shall initiate immediate action to prevent unauthorized access (e.g., secure room, change access codes, limit access, etc.).

Breach Investigation: The ICBHS Privacy Officer or designee shall be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with others in the department as appropriate. The Privacy Officer shall be responsible for all breach notification processes to the appropriate entities (DHCS, DHHS, media, law enforcement, etc.).

Upon receiving a report of a potential breach, the ICBHS Privacy Officer or designee will notify the Department of Health Care Services Privacy Officer immediately and provide a brief description of the potential breach. The DHCS Privacy Officer's contact information is privacyofficer@dhcs.ca.gov.

The ICBHS Privacy Officer or designee will forward the manager/ supervisor who reported the potential breach an ICBHS Privacy Incident Report. The manager/supervisor shall complete an ICBHS Privacy Incident Report and return it the Privacy Officer or designee within 48 hours.

Risk Assessment: Upon receipt of the ICBHS Privacy Incident Report, the ICBHS Privacy Officer will conduct a risk assessment to determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements. The ICBHS Privacy Officer will

perform a risk assessment based on at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the protected health information of to whom the disclosure was made.
- Whether the protected health information was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

Within 72 hours of the discovery of a potential breach, the ICBHS Privacy Officer or designee will complete a DHCS Privacy Incident Report and risk assessment and forward it to the DHCS Privacy Officer. DHCS will review and approve the determination of whether a breach occurred individual notification are required, and the corrective action plan.

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 the department 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.

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 associates 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.