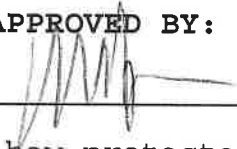


COUNTY OF IMPERIAL
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES

POLICY AND PROCEDURE MANUAL

SUBJECT: De-Identification of Protected Health Information (PHI)	POLICY: 01-80
SECTION: Administration	EFFECTIVE DATE: 4-14-03
REFERENCE: 45 C.F.R. Sections 164.502(d) & 164.514	PAGE: 1 of 5
AUTHORITY: 45 C.F.R. Part 164	SUPERSEDES: New Policy
	APPROVED BY: 

PURPOSE: To establish a policy that defines how protected health information (PHI) may be de-identified under the HIPAA Privacy Rule.

SCOPE: The information in this document applies to all members of the workforce which includes employees, contract employees, volunteers, trainees, etc., granted access to protected health information (PHI).

NOTES: The Health Insurance Portability And Accountability Act (HIPAA) Privacy Rule primarily addresses the protection of individually identifiable health information and specifies when such information can be used or disclosed. HIPAA allows a covered entity to de-identify health information by removing all identifying elements so that the remaining information cannot identify an individual and therefore is not subject to the protections specified for individually identifiable health information. 45 C.F.R. Section 164.502(d)(2) establishes requirements for uses and disclosures of de-identified information.

The preamble of the Privacy Rule discusses two ways to comply with de-identifying PHI. One method is the safe harbor method of de-identification; the other is statistical de-identification. Both methods are discussed below.

DEFINITIONS: **Authorized User:** An individual that is granted access to PHI for individuals through an authorization, IRB waiver or who is performing an activity related to health care operations.

De-identified Information: De-identified information means that providers have removed, coded, or encrypted data that identifies an individual. Health information that is de-identified, i.e., does not identify the individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual, is not PHI and therefore not subject to the requirements for the use and disclosure of PHI in the Privacy Rule,

Institutional Review Board (IRB): A committee composed of ICBHS personnel and community representatives with varying backgrounds and professional experience that review and approve research protocol on human subjects.

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.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the department, is under the direct control of the department, whether or not they are paid by the department.

POLICY: Imperial County Behavioral Health Services will de-identify health information whenever individually identifying information is not necessary to accomplish the intended purpose for the use or disclosure of health information or when use or disclosure of individually identifying information is not permitted by federal or state laws.

When use or disclosure of individually identifying information is necessary for public health, research, or health care operation activities, and the particular instance of use or disclosure is not permitted by federal or state laws, ICBHS will determine if a limited data set would meet the intended purpose of the use or disclosure. When a limited data set is deemed appropriate, ICBHS will enter into a data use agreement with the recipient of the information. (See Policy 01-81, Use and Disclosure of a Limited Data Set)

Requirements for De-identification of Protected Health Information

ICBHS may determine that health information is not individually identifiable using the safe harbor or statistical method of de-identification method of de-identification of PHI described below.

Safe Harbor Method of De-identification

Under the safe harbor method of de-identification, individual identifying information of the individual or of relatives, employers, or household members of the individual is rendered anonymous when the following identifying characteristics are completely removed. If these identifying characteristics are associated with health information, the information becomes individually identifying health information and must be protected from improper use or disclosure:

1. Names
2. Geographic subdivisions smaller than a state:
 - * street address
 - * city
 - * county
 - * zip code (except if by combining all zip codes with the same initial three digits, there are more than 20,000 people)
3. Names of relatives and employers
4. All elements of dates (except year) related to an individual including:
 - * birth date
 - * admission date
 - * discharge date
 - * date of death
 - * all ages over 89 and all elements including year indicative of such age except that such ages and elements may be aggregated into a single category of age 90 or older.
5. Telephone numbers
6. Fax numbers
7. Email addresses
8. Social Security Number (SSN)

9. BC number
10. Health beneficiary plan number
11. Account number
12. Certificate/License number
13. Vehicle identifiers, including license plate numbers
14. Device ID and serial number
15. Uniform Resource Locator (URL)
16. Identifier Protocol (IP) addresses
17. Biometric identifiers
18. Full face photographic images and other comparable images
19. Any other unique identifying number characteristic, code.

[45 C.F.R. 164.514(b)(2)(i)]

After removing the identifiers, the information cannot be released if ICBHS has actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

Protected health information used for research should be de-identified at the point of data collection for a research protocol approved by the Institutional Review Board, unless the participant voluntarily and expressly consents to the use of his or her personally identifiable information or an IRB waiver of authorization is obtained.

Statistical De-Identification

ICBHS may, as an alternative to de-identification, seek an expert opinion that disclosure of PHI would create minimal risk that the recipient would be able to identify the individual.

The expert must be a person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information

not individually identifiable.

The expert must apply those principles and methods to determine that the risk is very small that the information could be used, alone or in combination with any other reasonably available information, by an anticipated recipient to identify the individual who is the subject of the information.

The expert must document the method and results of the analysis to justify the determination. [45 C.F.R. 164.514(b)]

Re-identification

If an authorized user encrypts protected health information when creating de-identified information, the authorized user must ensure that:

1. The code or other means record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and,
2. No one involved in the de-identification process discloses the code or other means of record identification and does not disclose the mechanism to accomplish re-identification.

Enforcement

Management and supervisors are responsible for enforcing this policy and associated procedure(s). Members of the workforce who violate this policy or associated policies or procedures are subject to disciplinary actions appropriate to the nature of the violation in accordance with the ICBHS sanction policy.