	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 09** **PAGE** 1 **OF** 4 **EFFECTIVE DATE** June 10, 2016
POLICY: HIPAA POLICY **SP: Breach Reporting and Notification**		**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

To establish a process for reporting the impermissable or unauthorized acquistion, access, use or disclosure of Protected Health Information (PHI) in accordance with the requirements of Health Information Portability and Accountability Act (HIPAA).

DEPARTMENTS AFFECTED

All County agencies, departments, separate entities and Board-governed Special Districts that are determined to be covered by HIPAA.

DEFINITIONS

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

Breach: The acquistion, access, use or discloure of PHI in a manner not permitted by the HIPAA Privacy Rule.

Business Associate: A person or organization that on behalf of a covered entity, other than a member of the covered entity's workforce creates, receives, maintains, or transmits PHI.

Covered Entity: A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA covered transaction.

Disclosure: The release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

Health Care Component: County departments or programs that meet the definition of a Covered Entity or Internal Business Associate.

Health Insurance Portability and Accountability Act (HIPAA): A federal law designed to provide privacy and information security standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. (45 C.F.R. Parts 160 and 164)

Hybrid Entity: A single legal entity: (1) that is a Covered Entity; (2) whose business activities include both covered and non-covered functions; and (3) that designates Health Care Components.

Internal Business Associate: A County department or program that provides services to another County department or program covered by HIPAA that if it was a separate legal entity would fall within the definition of a Business Associate.

Privacy Officer: The person responsible for developing, implementing, and maintaining the County Privacy Policies and Procedures regarding the use and disclosure of PHI, responsible for receiving complaints under HIPAA, and for compliance with the HIPAA Privacy Rule.

Privacy Rule: Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. (45 C.F.R. Part 164 Subpart E).

Protected Health Information (PHI): Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium (excludes individually identifiable health information in employment records held by the Covered Entity in its role as employer).

Security Officer: The person responsible for the development and implementation of County policies and procedures as required by the HIPAA Security Rule.

Unsecured PHI: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of Health and Human Services (HHS) in the guidance issued under 42 U.S.C. section 17932, subdivision (h)(2).

PROCEDURES

When a breach of unsecured PHI is discovered, the County HIPAA Privacy Officer and the County HIPAA Security Officer must be notified immediately.

The County will notify affected individuals, the U.S. Department of Health and Human Services (HHS), and the media, where required, of any breach of unsecured PHI. All suspected breaches of unsecured PHI will be investigated, and all necessary notifications will be sent, in accordance with the guidelines set forth in this standard.

A. **Notification to Individuals:**

1. Notification must be made to the affected individuals without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

2. Method of Notification. Notification must be made through one of the following methods:

   a. *Written notice*.

      i. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

      ii. If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

   b. *Substitute notice*.

      i. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (A)(2)(a)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (A)(2)(a)(ii).

      ii. In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

iii. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

1. Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

2. Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may have been included in the breach.

c. *Additional notice in urgent situations*. In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (A)(2)(a) of this section.

3. Notification shall include:

a. A brief description of what happened, including the date of breach and the date of discovery of the breach, if known;

b. A description of the types of unsecured PHI that were involved in the breach, e.g. full name, social security number, date of birth, home address, diagnosis, or other types of information that were involved;

c. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

d. A brief description of what the department is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches;

e. Contact procedures for individuals to ask questions or learn additional information which shall include a toll-free number, an email address, website, or postal address;

f. The notification shall be written in plain language and if necessary, translated into an alternative language if translation is required for the patient.

B. **Notification to Health and Human Services (HHS)**:

1. For breaches involving less than 500 individuals, the department shall maintain a log or other documentation of such breaches, and not later than 60 days after the end of each calendar year, provide the notification required to HHS in the manner specified on HHS website.

2. For breaches involving 500 or more individuals, the department shall provide the notification required, contemporaneously, with the notice required to the individuals and in the manner specificed on the HHS website.

C. **Notification to Media**:

1. For breaches involving 500 or more individuals, in accordance with HIPAA, the department will ensure that a prominent media outlet is notified without reasonable delay and in no case later than 60 calendar days after discovery of a breach. HCC departments shall consult with their

assigned Deputy County Counsel prior to posting notification to the media and shall inform the County Public Information Officer.

2. The notication to the media shall contain the same required elements as Notice to Individuals.

D. **Law Enforcement Delay:**

If a law enforcement official states that a required notification, notice, or posting would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

This Policy shall not be construed as relieving departments of their responsibility to develop full and complete departmental policies, procedures, and practices necessary to expand and tailor this overall County Policy to the particular needs of their departments.

LEAD DEPARTMENT
Human Resources