	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 05** **PAGE** 1 **OF** 3 **EFFECTIVE DATE** June 10, 2016
POLICY: HIPAA POLICY **SP: Risk Analysis and Management**		**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

To establish guidelines to regularly identify, evaluate, document and manage potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI).

DEPARTMENTS AFFECTED

All County agencies, departments and Board-governed Special Districts that are determined to be covered by the Health Insurance Portability and Accountability Act (HIPAA).

DEFINITIONS

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 Protected Health Information (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.

Electronic Protected Health Information (ePHI): Protected health information in electronic form.

Health Care Component (HCC): 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)

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.

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 Covered Entity in its role as employer).

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).

Risk: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets.

Risk Analysis: An accurate and thorough assessment that:

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;

- Prioritizes risks; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.

Risk Management: A process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

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

Security Rule: Establishes national standards to protect individuals' ePHI that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. (45 C.F.R. Part 160, and Part 164 Subparts A and C.)

Threat: The potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:

- Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
- Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
- Natural – fires, floods, electrical storms, tornadoes, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
- Other – explosions, medical emergencies, misuse of resources, etc.

Vulnerability: Flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the Security Rule.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or internal business associate, is under the direct control of such covered entity or internal business associate, whether or not they are paid by the covered entity or internal business associate.

PROCEDURES

A. Health Care Component (HCC) departments that maintain or transmit ePHI shall:

1. Conduct and document a thorough risk analysis a minimum of every three (3) years.

2. Conduct additional risk analyses in the following instances:

    a. Prior to the purchase or integration of new technologies.

    b. Prior to changes being made to physical safeguards.

    c. Following the occurrence of an event or incident warranting the reevaluation of risks, which requires an immediate risk analysis.

3. Include the following minimum components in the risk analyses and management strategies:

    a. Asset inventory – identify where ePHI is created, received, maintained, processed, or transmitted;

b. Threat identification and assessments – identify and document potential threats;

c. Determination of risk exposures – develop a list of technical and non-technical system vulnerabilities that could be exploited or triggered by the potential threat-sources; and,

d. Development of a risk management strategy

i. Likelihood determination – determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited.

ii. Impact analysis – determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability.

iii. Control recommendations – identify controls that could reduce or eliminate the identified risks, as appropriate to the HCC departments operations to an acceptable level.

iv. Control analysis – document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the HCC department to minimize or eliminate the likelihood of a threat-source exploiting a system vulnerability.

v. Develop a risk management plan – develop an overall action plan to prioritize and implement the controls identified.

4. Maintain a written record of the analysis for six (6) years.

5. Submit the risk analysis findings and the management strategy to the County HIPAA Privacy Officer and County HIPAA Security Officer within 30 days of concluding the analysis.

6. Implement measures to remediate vulnerabilities and sufficiently reduce risk exposure within 90 days of concluding their assessment. If a specific vulnerability cannot be remediated within the allotted time due to business or technology constraints, a written extension request must be submitted to the County HIPAA Security Officer for approval.

7. Document the remediation activities. Provide follow-up to the County HIPAA Security Officer for the remediation activities completed within 90 days. Provide regular status updates to the County HIPAA Security Officer for remediation activities that were granted an extension.

B. Documented risk analyses and management plans shall be kept confidential, unless disclosure is required by law.

C. All workforce members are expected to fully cooperate with all persons charged with performing a risk analysis or engaging in risk management. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation.

This Standard Practice 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