DEPARTMENTAL GUIDEBOOK TO THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA Guidebook 2018

Last Revised 12.28.17

HIPAA GUIDEBOOK

This HIPAA Guidebook gives instruction on how departments and programs are to operate under countywide HIPAA standards. The Guidebook sets forth minimum standards and expectations for departments and programs. Departments and programs must implement specifically tailored HIPAA standards and procedures to reflect the status and needs of the individual department and program.

TABLE OF CONTENTS

TERMINOLOGY

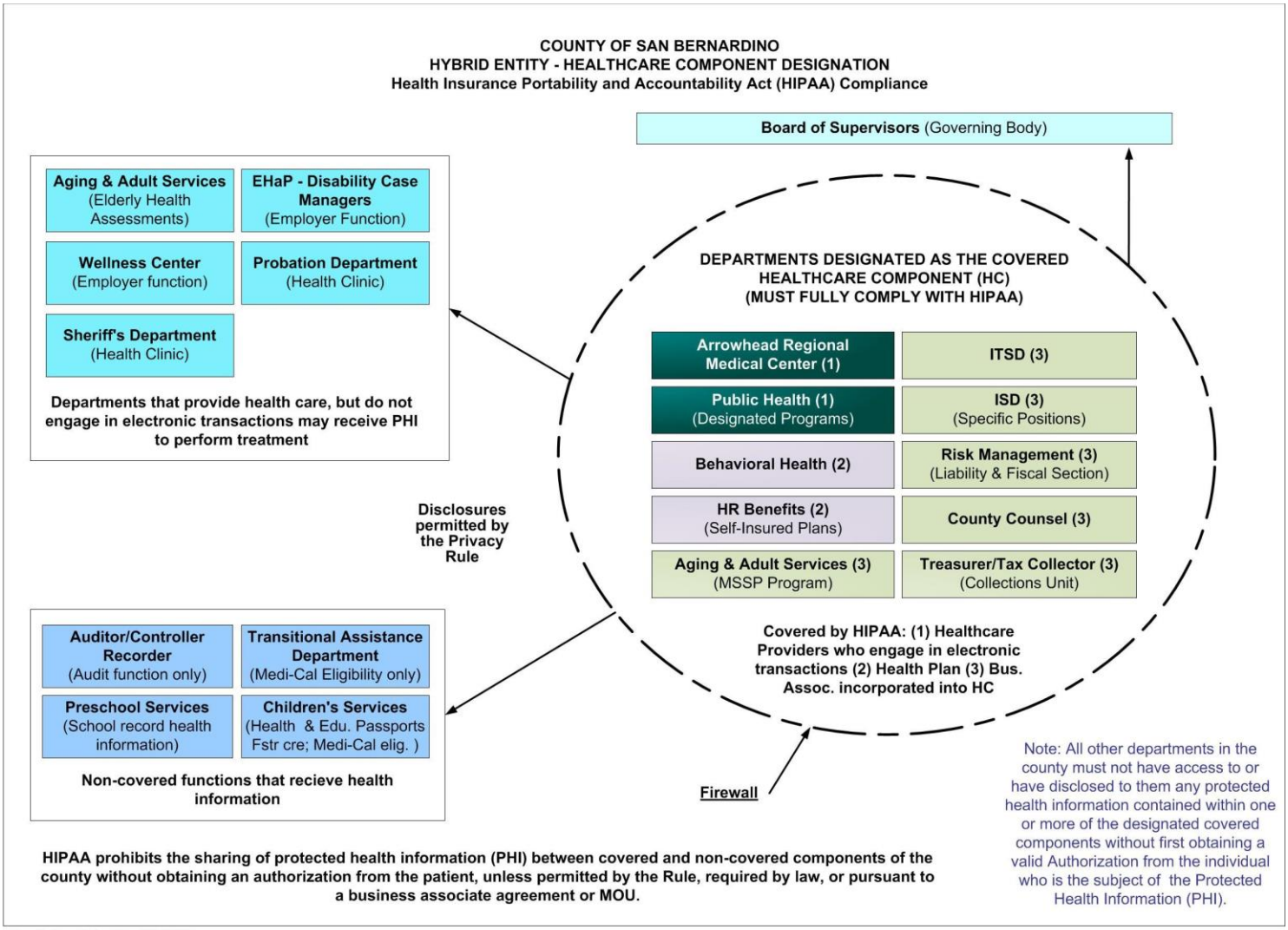
Breach	The acquisition, access, use or disclosure of Protected Health Information (PHI) in a manner not permitted by the HIPAA Privacy Rule.
Business Associate	A person or organization that, on behalf of a covered entity other than a member of the covered entity's workforce, creates, receives, maintains 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.
Healthy 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)
Health Information Technology for Economic and Clinical Health (HITECH) Act	Enacted as part of the American Recovery and Reinvestment Act of 2009, it was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. (45 CFR Part 160, subpart D.)
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).
Risk Assessment	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.

COUNTY HEALTH CARE COMPONENT

The County is designated as a hybrid entity, as defined by 42 C.F.R. section 164.103. This means the County has business activities that include both functions that are covered by HIPAA, and functions that are not covered by HIPAA. Covered functions are declared to be a part of the hybrid entity's "Health Care Component." 42 C.F.R. section 164.105 requires a hybrid entity to ensure that each of its health care components complies with HIPAA. In order to comply with this section, in 2016 and 2017, the County conducted a survey of all departments and programs to re- determine which departments and programs must be included in the Health Care Component. Based upon the survey results, the Chief Executive Officer approved County Standard Practice 14-03SP01, declaring the following department to be designated as the County's Health Care Component:

- Arrowhead Regional Medical Center (ARMC)
- Auditor/Controller-Treasurer-Tax Collector—Central Collections
- Board of Supervisors
- County Administrative Office
- County Counsel
- Department of Aging and Adult Services (DAAS) - Multipurpose Senior Services Program
- Department of Behavioral Health (DBH)
- Department of Public Health (DPH)
- Human Resources—Employee Benefits and Services Division
- Information Services Department (ISD)
- Risk Management

A chart identifying the Health Care Component and its relationship to other County departments is provided on the following page. The detailed survey results for all departments are included here as Appendix A.



Revision 4.1 - April 2015
by Collin Goodrum, ARMC Hospital Privacy & Security Officer

COUNTY POLICY AND STANDARD PRACTICES

In an effort to comply with the HIPAA Final Rule and adopt a countywide HIPAA Program, the Board of Supervisors approved County Policy 14-03 on July 28, 2015. The Policy designates the County as a hybrid entity for purposes of HIPAA, declares that the County is committed to protecting the privacy of protected health information (PHI) which it creates, receives, maintains and transmits, and directs the County to comply with certain steps in order to comply with HIPAA. The steps were addressed in separate Standard Practices, which together with the Policy, are included in this Guidebook as Appendix B. The Policy and Standard Practices include:

- 14-03 Health Insurance Portability and Accountability Act (HIPAA) Policy
- 14-03 SP01 Health Care Component Designation
- 14-03 SP02 Privacy Officer and Security Officer
- 14-03 SP03 Administrative, Technical and Physical Safeguards
- 14-03 SP04 Workforce Training
- 14-03 SP05 Risk Analysis and Management
- 14-03 SP06 Uses and Disclosures of Protected Health Information
- 14-03 SP07 Patient Privacy Rights
- 14-03 SP08 Business Associate Agreements
- 14-03 SP09 Breach Reporting and Notification
- 14-03 SP10 HIPAA Complaint Process

The Standard Practices set forth minimum requirements for the County departments and programs. Departments and programs are required to implement policies and procedures specific to their department that are in addition to, and do not conflict with, the Standard Practices.

DEPARTMENT RESPONSIBILITIES

Departments and programs that are covered by HIPAA and designated as part of the County's Health Care Component must complete the following steps:

- Decide on and document an organizational structure. For departments that are hybrid entities, the department must designate themselves as a hybrid entity and declare which programs fall within the department's health care component. [14-03 SP01.]
- Designate a HIPAA Privacy Officer and a Security Officer. [See 14-03 SP02.]
- Develop and implement policies and procedures indicating the administrative, technical and physical safeguards put in place for the protection of PHI in compliance with HIPAA and the County Policy and Standard Practices. If policies and procedures are already in place, review to ensure compliance with the current requirements of HIPAA and the County Policy and Standard Practices. [See 14-03 SP03.]
- Train workforce on the requirements of HIPAA, utilizing the County HIPAA training. [See 14- 03 SP04.]
- Conduct a HIPAA Risk Assessment. [14-03 SP 05.]
- Review and assess the current use and disclosure practices for PHI and compare with the County Policy and Standard Practices in addition to the HIPAA Privacy Rule and Security Rule requirements. Ensure current practices comply with the minimum necessary provisions. [14- 03 SP06.]
- Identify Business Associate relationships and enter into Business Associate Agreements utilizing the County Business Associate Agreement template (see Appendices C and D). [14-03 SP08.]
- Develop a departmental Notice of Privacy Practices, using the County template Notice of Privacy Practices as a baseline (see Appendix E). [14-03 SP07.]
- Develop a system to track and account for disclosures. If a system is already in place, review the system to ensure it meets current HIPAA requirements. [14-03 SP07.]
- Provide for individual's rights to access and amend his/her PHI. [14-03 SP07.]
- Ensure a breach reporting system is in place to immediately react to suspected and actual breaches of PHI. [14-03 SP09.]
- Develop a HIPAA Complaint Process. [14-03 SP10.]

BUSINESS ASSOCIATE GUIDELINES

The identification and documentation of business associate relationships is a key aspect of HIPAA compliance. A business associate is defined as a person who on behalf of a covered entity, creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, or provides the covered entity with a covered service there the provision of the service involves the disclosure of PHI from the covered entity to the person. To determine if a contractor is a business associate, consult Appendix C Business Associate Flow Chart.

County Standard Practice 14-03 SP08 lays out the requirements for Departments with regard to business associates. One such requirement is that departments must identify their business associate relationships, and document such relationship through a Business Associate Agreement. A template Business Associate Agreement has been formulated and is included as Appendix D. Departments are required to use the template unless authorized to modify. Contractor provided business associate agreements may be utilized with County Counsel review and approval.

Departments may be business associates with another County department. For purposes of the County HIPAA Policy and related Standard Practices, the departmental business associate is referred to as an “internal business associate.” Internal business associates have been identified as part of the County Health Care Component and include: Risk Management, County Counsel, ISD, and Central Collections. A formal business associate agreement is not required between a department and an internal business associate, however, a memorandum of understanding must be instituted to dictate responsibilities and expectations of both departments.

APPENDIX A

COUNTY SURVEY RESULTS

County of San Bernardino HIPAA HCC Designation Chart

Entity	Contact	Included in HCC (Yes/No)	Notes	HIPAA Reference[1]
Aging and Adult Services	Chris Tarr	Yes	Multipurpose Senior Services Program (MSSP) is a covered entity and business associate.	45 CFR §§ 160.102(a) & 160.103
Agriculture/Weights & Measures	Roberta Willhite	No	Not a health plan, healthcare clearinghouse or provider	
Airports	Elvia Hernandez	No	Not a health plan, healthcare clearinghouse or provider	
Arrowhead Regional Medical Center (ARMC)	Collin Goodrum	Yes	Acute Care Hospital – Health Care Provider	45 CFR §§ 160.102(a) & 160.103
Assessor-Recorder-Clerk	Lisa Nickel	No	Not a health plan, healthcare clearinghouse or provider Recorder collects Vital Statistics information, but not a CE	164 CFR § 512(b)(1)(i)
Auditor-Control/Treasurer-Tax Collector	Vanessa Doyle	Yes	Internal business associate providing collections services to ARMC. Collections is the only covered component.	45 C.F.R. § 160.103
Behavioral Health (DBH)	Marina Espinosa	Yes	Health Care Provider and Health Plan	45 CFR 160.102(a) & 160.103
Board of Supervisors	Josefina Kenline	Yes	Governing body of all components of the HCC, therefore member of the workforce.	45 CFR §§ 160.103 and 164.530
Child Support Services	Marci Jensen-Eldred	No	Not a health plan, healthcare clearinghouse or provider	
Children's Network	Kathy Turnbull	No	Not a health plan, healthcare clearinghouse or provider	
Children & Family Services	Christine Chavez	No	Not a health plan, healthcare clearinghouse or provider. Pay for care through Child Abuse	

[1] For Departments that are not identified as falling under the requirements of HIPAA, no HIPAA reference is provided.

Entity	Contact	Included in HCC (Yes/No)	Notes	HIPAA Reference[1]
			Treatment Services but not an insurance plan.	
Clerk of the Board	Lynna Monel	No	Not a health plan, healthcare clearinghouse or provider	
County Administrative Office (CAO)	Dena Smith	Yes	Provides administrative support for HCC departments and has access to PHI.	45 CFR §160.103
County Counsel	Robin Simon	Yes	Internal Business Associate – Provides legal representation to covered entities and business associates	45 CFR 160.103(1)(ii)
County Library	Leonard Hernandez	No	Not a health plan, healthcare clearinghouse or provider	
County Museum	Leonard Hernandez	No	Not a health plan, healthcare clearinghouse or provider	
District Attorney	Dan Silverman	No	Not a health plan, healthcare clearinghouse or provider.	
Economic Development Agency (EDA)	Larry Vanpel	No	Not a health plan, healthcare clearinghouse or provider	
Facilities Management	Bill Ogg	No	Not a health plan, healthcare clearinghouse or provider. Employees do access facilities where PHI is stored and will be required to sign confidentiality statements.	
Fire	Mike Sadsad and Christine Tennorio	No	Provide first responder services and initial treatment provider. Also bill Medi-Cal and Medicare through third party billing contractor for services provided. Fire is a separate legal entity and therefore will act as its own hybrid entity.	45 CFR § 160.102

Entity	Contact	Included in HCC (Yes/No)	Notes	HIPAA Reference[1]
Fleet Management	BJ Cruz	No	Not a health plan, healthcare clearinghouse or provider	
Human Resources	Yvonne Johnson	Yes	Covered Entity Self-funded health plan – HR Employee Benefits	45 CFR 160.102(a) and 160.103, 164.501, 164.504(f)
Human Services Administration	Monique Perez	ROQS – No HS Auditing – No PDD - No PID – No ASD - No	Some HS divisions may have access to health information, however it is not PHI within the meaning of HIPAA and no business associate function is being provided.	
IHSS/Public Authority	Rosa Hidalgo	No	Not a health plan, healthcare clearinghouse or provider	
Information Services Dept. (ISD)	Jennifer Hilber	Yes	Internal Business Associate - Provides technical support to covered entity departments	45 CFR 160.103
ITSD	Danny Tillman	No	Not an internal business associate, does not have access to PHI.	45 CFR §160.103
Land Use	Lanta Manalili	No	Not a health plan, healthcare clearinghouse or provider	
Preschool Services	Phalos Haire	No	Not a health plan, healthcare clearinghouse or provider	
Probation	Alice Rivera	No	Medical services pays for medical care, but not a health plan. Receives PHI from ARMC under the correctional institution exemption. Follow up on health clinic and billing	45 CFR 164.512(k)(5)
Public Defender	Phyllis Morris	No	Not a health plan, healthcare clearinghouse or provider	
Public Guardian	Chris Tarr	No	Not a health plan, healthcare clearinghouse or provider	

Entity	Contact	Included in HCC (Yes/No)	Notes	HIPAA Reference[1]
Public Health (DPH)	Ken Johnston	Yes	Health care provider, programs include: Clinic Operations (including FQHCs), CCS, Family Health Services, DPH Administration, Compliance Unit, Fiscal and Administrative Services, Information Services and Laboratory	45 CFR 160.102
Public Works	Gerry Newcombe	No	Not a health plan, healthcare clearinghouse or provider	
Purchasing	Lisa Brazfield	No	Not a health plan, healthcare clearinghouse or provider	
Real Estate (Includes Architecture & Engineering and PMD)	Terry Thompson	No	Not a health plan, healthcare clearinghouse or provider	
Regional Parks	Maureen Snelgrove	No	Not a health plan, healthcare clearinghouse or provider	
Registrar of Voters	Renee McMillon	No	Not a health plan, healthcare clearinghouse or provider	
Risk Management	Rafael Viteri	Yes	Internal Business Associate – Business associate to ARMC, DPH and DBH (Liability and Fiscal)	45 CFR 160.103 Bus. Assoc. (1)(i) and (ii)
Sheriff (includes Coroner)	Terry Fillman	No	Health clinic provides healthcare for incarcerated adults, but does not bill Medicaid/Medicare. Receives PHI from ARMC under the correctional institution and law enforcement exemption.	45 CFR 160.102 45 CFR 160.102(a) & 164.512(k)(5)
Special Districts	Mary Mayes	No	Not a health plan, healthcare clearinghouse or provider	

Entity	Contact	Included in HCC (Yes/No)	Notes	HIPAA Reference[1]
Transitional Assistance Department (TAD)	Elaine Angley	No	Provide eligibility determinations under Medi-Cal, exemption exists	45 CFR 160.103 Bus. Assoc. (4)(iii) and 45 CFR 164.512(k)(6)
Veteran's Affairs	Frank Guevara	No	Include PHI in claims for disability and pension, but are not acting as a business associate or covered entity in that role.	
Workforce Development (WDD)	Bradley Gates	No	Not a health plan, healthcare clearinghouse or provider	

APPENDIX B
COUNTY HIPAA POLICY AND STANDARD PRACTICE

	COUNTY OF SAN BERNARDINO **POLICY MANUAL**	**No. 14-03** **PAGE** 1 **OF** 2 **EFFECTIVE DATE** July 28, 2015
POLICY: HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) POLICY		**APPROVED** JAMES RAMOS Chairman, Board of Supervisors

POLICY STATEMENT AND PURPOSE

To define and document the County of San Bernardino's Health Insurance Portability and Accountability Act (HIPAA) Compliance Program. The program shall identify the covered Health Care Component (HCC), establish minimum compliance standards for the covered HCC, and designate a County Privacy Officer and a County Security Officer.

DEPARTMENTS AFFECTED

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

DEFINITIONS

Breach: The acquisition, access, use or disclosure of Protected Health Information (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.

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 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 Protected Health Information, responsible for receiving complaints under HIPAA, and for compliance with the HIPAA Privacy Rule.

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).

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

POLICY AMPLIFICATION

The Board of Supervisors designates the County of San Bernardino as a Hybrid Entity for purposes of HIPAA. The County is committed to protecting the privacy of PHI which it creates, receives, maintains, and transmits. To comply with HIPAA, the County will:

1. Designate the County's Health Care Component.
2. Designate a County Privacy Officer.
3. Designate a County Security Officer.
4. Create and maintain policies and procedures for the protection of PHI in written or electronic form.
5. Establish administrative, physical, and technical safeguards for protecting PHI.
6. Implement and oversee workforce training on privacy and security policies and procedures.
7. Establish a formal complaint process.
8. Establish and enforce a risk assessment process.
9. Refrain from retaliating against an individual for exercising their rights under HIPAA (whistleblower, filing a complaint, etc).
10. Establish a process to report breaches of PHI as required by law.

Nothing in this Policy shall 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

APPROVAL HISTORY
Adopted 11/18/08; Item Number 86; Amended 07/28/15; Item Number 41.

REVIEW DATES
July 2020

	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 01** **PAGE** 1 **OF** 2 **EFFECTIVE DATE** June 10, 2016
POLICY: HIPAA POLICY **SP: Health Care Component Designation**		**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

To designate which departments are included in the Health Care Component (HCC) and ensure that all departments within the designated HCC of the County comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

DEPARTMENTS AFFECTED

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

Compliance Oversight Committee: The Compliance Oversight Committee serves to safeguard confidential information maintained by the County of San Bernardino through collaborative compliance management, risk mitigation and opportunity management efforts. The Committee, comprised of delegates from County departments, divisions, and agencies is responsible for: examining and monitoring compliance with codes, regulations and requirements related to the protection of confidential information; monitoring the risk assessment of systems that contain sensitive and confidential information, including recommendations for mitigating areas of risk; the recommendation of policies and standard practices relating to the privacy and security of confidential information; and the implementation and oversight of compliance with County policies and standard practices related to confidential information. Committee delegates meet regularly to share security, risk and internal control knowledge to achieve best practices on countywide.

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.

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 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).

PROCEDURES

A. HCC Departments

The following departments are designated as part of the HCC:

1. Arrowhead Regional Medical Center
2. Auditor/Controller-Treasurer-Tax Collector – Central Collections
3. County Counsel
4. Department of Aging and Adult Services – Multipurpose Senior Services Program
5. Department of Behavioral Health
6. Department of Public Health
7. Human Resources - Employee Benefits and Services Division
8. Information Services Department
9. Human Services - Information Technology and Support Division
10. Risk Management

Departments designated as part of the HCC shall assign a representative to the County Compliance Oversight Committee. The representative shall participate regularly in the County Compliance Oversight Committee meetings.

Any department that is not designated above as part of the HCC, but at a later date falls within the definition of a Covered Entity or Internal Business Associate, shall be considered as part of the HCC and shall comply with the requirements of County Policy 14-03 and the related Standard Practices.

B. Use and Disclosure Restrictions

Departments within the HCC cannot disclose PHI to a non-HCC department of the County without appropriate authorization or as permitted by the Privacy Rule.

1. Non-HCC departments that create or receive PHI from an HCC department shall only use or disclose that information in a manner consistent with the Privacy Rule.

2. If an employee performs duties for both an HCC department and a non-HCC department, they shall only use or disclose PHI created or received in the course of their work with the HCC department in a manner consistent with the Privacy Rule.

LEAD DEPARTMENT
Human Resources

PURPOSE

To define and delineate the responsibilities of the County Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer, HIPAA Security Officer and Department Privacy Officer and Department Security Officer.

DEPARTMENTS AFFECTED

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

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

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).

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 Privacy 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 Privacy 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 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.

Security Rule: Establishes national standards to protect 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.

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

The Chief Executive Officer is responsible for appointing a County HIPAA Privacy Officer and a County HIPAA Security Officer.

A. County HIPAA Privacy Officer

The HIPAA Privacy Officer, at a minimum, shall:

1. Preside as Chair of the Compliance Oversight Committee,

2. Implement and monitor compliance with the County policies and standard practices adopted to comply with the HIPAA Privacy Rule, including policies and standard practices that address:

    a. Patient Privacy Rights

    b. Minimum Necessary Standard

    c. Administrative, Physical and Technical Safeguards

    d. Workforce Training

    e. Complaint Process

    f. Business Associate Contract Requirements

    g. Permitted Disclosures

    h. Breach Reporting

    The Privacy Officer shall be responsible for recommending the adoption of new policies and standard practices, or the revision of existing policies and standard practices regarding compliance with HIPAA, when necessary to comply with changes to the law or best practices.

3. Establish, implement, and amend as necessary, a process for individuals to make complaints related to HIPAA, the entity's policies and procedures, or the entity's privacy notices, and designate a person or office to receive those complaints;

4. Ensure subpoenas and requests for amendment to a health record that affect multiple departments are coordinated and disseminated to the appropriate departments;

5. Implement and monitor compliance with workforce training on privacy policies, standard practices and procedures;

6. Implement and monitor compliance with the County policies and standard practices that require management to establish, apply and document sanctions against workforce members who violate the law or the County's privacy policies and procedures;

7. Implement and monitor compliance with the County policies and standard practices that require mitigation of any harmful effects that result from the unlawful disclosure of PHI;

8. Maintain required policies and procedures in written or electronic form;

9. Direct and oversee the County breach reporting process and notification requirements, including performing the required privacy breach notification risk analysis pursuant to law; and

10. Ensure that the following records are kept in writing or electronically, pursuant to statutory requirements:

    a. Required policies and procedures;

    b. Communications required to be in writing; and,

    c. Any action, activity, or designation required to be documented.

B. County's HIPAA Security Officer

The HIPAA Security Officer, at a minimum, shall:

1. Implement and monitor compliance with the County policies and standard practices to comply with the HIPAA Security Rule, and recommend amendments to them as necessary to comply with changes in the law;

2. Define and implement the necessary administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of ePHI the County creates, receives, maintains or transmits;

3. Ensure safeguards are in place to protect ePHI against any reasonably anticipated threats or hazards to the security or integrity of the information;

4. Ensure safeguards are in place to protect ePHI against any reasonably anticipated uses or disclosures that are not permitted or required under the Privacy Rule; and,

5. Require compliance by workforce members.

C. The County HIPAA Privacy Officer and the County HIPAA Security Officer shall work together to ensure their respective policies and procedures do not conflict with each other. They will also work with HCC departments to assist the HCC department to comply with the Privacy Rule and Security Rule.

D. Department Privacy Officer and Department Security Officer

1. HCC departments shall appoint a privacy officer and a security officer who shall be responsible for the privacy and security program development, implementation, maintenance, oversight and compliance within their departments. In some departments, the Privacy Officer and the Security Officer might be the same person.

2. HCC department privacy officers and security officers are required to submit an annual report to the County HIPAA Privacy Officer detailing the status of the health information privacy and security program within their respective departments. The County HIPAA Privacy and Security Officers will establish the format and deadline for report submissions.

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

	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 03** **PAGE** 1 **OF** 9 **EFFECTIVE DATE** June 10, 2016
POLICY: HIPAA POLICY **SP: Administrative, Technical and Physical Safeguards**		**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

To document minimum administrative, technical and physical safeguards applicable to the County's Health Care Component (HCC) in order to minimize the risk of unauthorized access, use or disclosure of Protected Health Information (PHI).

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

Administrative Safeguards: Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect PHI and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

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.

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

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.

Physical Safeguards: Physical measures, policies and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

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).

Technical Safeguards: The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Unsecured PHI: Protected health information 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 in the guidance issued under 42 U.S.C. Section 17932 subdivision (h)(2).

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

Departments within the HCC must comply with the minimum administrative, technical and physical safeguards detailed below. Departments shall implement reasonable and appropriate safeguards specific to their department that are in addition to and do not conflict with the safeguards contained in this Standard Practice (SP).

Administrative Safeguards

A. Security Management Process: HCC departments must comply with the following safeguards to prevent, detect, contain and correct security violations.

1. Risk Analysis: Departments shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the department. Departments shall conduct such a risk assessment of systems containing ePHI at the time of procurement and at any time there is a substantial change to the system thereafter. Departments shall conduct an overall assessment at a minimum every three (3) years.

2. Risk Management: Departments shall adopt and maintain a risk management plan sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the following:

    a. Ensure the confidentiality, integrity, and availability of all ePHI the department creates, receives, maintains, or transmits.

    b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

    c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA.

    d. Ensure compliance with HIPAA by the department's workforce.

3. Sanction Policy: Employees who fail to comply with the security policies and procedures of the County and the department shall be disciplined in accordance with Human Resources policies and County Personnel Rules. Departments shall have policies and procedures that address the sanctions applicable to violations of HIPAA.

4. Information System Activity Review: Departments shall regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

B. Assigned Privacy and Security Responsibility: Departments are required to identify a privacy officer and a security officer within the department who are responsible for the development and implementation of the policies and procedures required by County Policy, Standard Practices and HIPAA for the Department.

C. Workforce Security: Departments shall implement policies and procedures to ensure that all members of the department's workforce have appropriate access to PHI, and to prevent those workforce members who should not have access from obtaining access to PHI.

1. Authorization and/or Supervision: Only those employees necessitating access to PHI to fulfill a job function shall be authorized to access PHI. Managers and/or supervisors are required to supervise employees granted access to PHI to ensure the employees are utilizing their access correctly and only for assigned job functions. Departments shall implement procedures for the authorization and/or supervision of workforce members who work with PHI or in locations where it might be accessed.

2. Workforce Clearance Procedure: Upon hire of an employee and at regular intervals thereafter, the department shall determine the appropriate level of access to PHI to be granted to the employee. Any workforce member must undergo a background check prior to being granted access to PHI. Only the minimum level of access shall be granted for the assigned job function. Employees are only authorized to view PHI pursuant to a stated job function and shall only view the minimum amount necessary to fulfill the job function. Departments shall implement procedures to determine that the access of a workforce member to PHI is appropriate.

3. Termination Procedures: Access to PHI shall be terminated promptly upon departure of an employee or when assigned job duties that no longer require access to PHI. Departments shall implement procedures for terminating access to PHI in such circumstances.

D. Information Access Management: Departments shall implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of the HIPAA Privacy Rule.

1. Access Authorization: Each department must ensure that only workforce members who require access to information are granted access. Departments are responsible for ensuring that the access to information granted to workforce members is the minimum necessary required for individual job roles and responsibilities. Access to information must be granted upon a demonstrable and valid "need-to-know" basis and not merely by position or title. If the workforce member no longer requires access, the department must complete the necessary process to terminate access in a timely fashion. Departments must implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process or other mechanism.

2. Access Establishment and Modification: Departments shall establish and document authorizations granted for a workforce member's access to workstations, transactions, programs, processes and systems. Departments shall regularly review and modify a workforce member's right of access to any workstation, transaction, program, process or system that contains ePHI to ensure access remains necessary. Departments shall review access granted to all systems, programs, and processes containing ePHI at regular intervals to ensure only authorized individuals maintain access.

3. Access of ePHI: Workforce members are prohibited from accessing ePHI from a public computer, a public wireless network, or an unsecured wireless network, unless a secure process that has been authorized by the department is utilized. ePHI shall not be accessed from a personal mobile device unless a secured process that has been approved by the department is utilized. Departments shall implement policies and procedures to control access of workforce members' use of the San Bernardino County Outlook Web App (webmail), Virtual Private Networks (VPN) and other remote access technologies to prevent unauthorized access to ePHI from public and personal devices. Departments shall implement policies and

procedures concerning the telecommuting of workforce members, to ensure ePHI is accessed in a secure, authorized and appropriate manner.

E. Privacy and Security Awareness and Training:

1. Training*:* Before access is granted to PHI, workforce members shall receive training on the privacy and security requirements of HIPAA and the County and department policies established thereunder in accordance with Standard Practice 14-03 SP04.

2. Security Reminders: Departments shall conduct periodic security reminders for all workforce members granted access to PHI no less than every year.

F. Privacy and Security Incident Procedures: Departments shall implement policies and procedures for responding to privacy and security incidents. Policies must address incident reporting, mitigation, documentation, response timeframes and procedures, compliance with applicable state and federal reporting requirements, retention of reports and documentation, and sanctions.

G. Contingency Plan: Departments shall establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI. HCC departments shall comply with the following:

1. Data Backup Plan: Establish and implement procedures to create and maintain retrievable exact copies of ePHI.

2. Emergency Mode Operation Plan: Establish procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

3. Disaster Recovery Plan: Establish procedures to restore any loss of data and normal business processes.

4. Testing and Revision Procedures: Implement procedures for periodic testing and revision of contingency plans.

5. Applications and Data Criticality Analysis: Assess the relative criticality of specific applications and data in support of other contingency plan components.

H. Evaluation: Departments shall perform a periodic technical and nontechnical evaluation of security controls and policies and procedures that affect the security of PHI and the systems that contain it.

Physical Safeguards

A. Facility Access Controls: Physical access to electronic information systems and facilities in which the electronic information systems are housed must be limited to only those authorized to access the system or facility.

1. Contingency Operations: Departments must establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

2. Facility Security Plan: Departments must implement policies and procedures to safeguard their facilities and the equipment therein from unauthorized physical access, tampering, and theft. At a minimum the policies and procedures must include the following:

    a. Facilities containing PHI are secured through the use of entry by ID badge, key card or other secure method to prevent unauthorized access.

b. Keypads/cipher locks are changed periodically.

c. Computer server rooms are secured from unauthorized access. Access must be permitted and documented in such a way as to provide sufficient audit trail capability.

d. Workforce members shall not allow entry into a secure facility to an unauthorized individual.

3. Access Control and Validation Procedures: Departments must implement procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revisions. At a minimum the policies and procedures must include the following:

   a. Departments must ensure that workforce members surrender ID badges promptly after termination or upon departure from the department.

   b. Workforce members must report lost/stolen badges immediately and shall not share ID badges.

   c. Departments shall periodically review access granted to facilities to ensure access remains appropriate.

   d. Documentation of visitor controls, including the use of sign-in/sign-out sheets, physical escort of visitors through the facility and no visitors left unattended in areas where PHI is located or stored.

4. Maintenance Records: Departments must implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security.

B. Workstation Use and Security: Departments must implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI. Departments must further implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users. At a minimum departments must require:

1. Workstations must be used in an appropriate and authorized manner. Workforce members must use workstations to support clinical, research, education, administrative and other legitimate functions of the department.

2. Workforce members have no expectation of privacy when using department systems and workstations. The County may log, review or monitor any data contained within or transmitted by any County owned information system, technology device or equipment.

3. Access to workstations must be controlled by requiring authentication using a User ID and a password or an access device (e.g., token, fingerprint readers), unless specifically exempted and authorized by the department.

4. Workforce members must report suspected unauthorized access/use of a workstation or the loss or theft of a workstation immediately.

5. Workforce members must lock or log off of the workstation before leaving the workstation unattended for any period of time.

6. Workstations must be positioned or protected from view so that ePHI is not visible to unauthorized persons.

7. Workstations and peripheral devices must be secured in areas not accessible by unauthorized workforce members or other unauthorized personnel or individuals.

8. On a periodic basis the risk to workstations containing ePHI must be assessed to determine the level of physical protection required.

9. Portable workstations must be physically protected at all times, including while traveling.

10. PHI may not be stored on a portable workstation unless it is protected either through encryption or an equivalent protection method.

C. Device and Media Controls: Departments must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility. Media can be any storage device or medium which is used to store in any way ePHI, including, but not limited to, CDs, DVDs, thumbdrives, floppy disks, cell phones, wireless devices and external hard drives.

1. Disposal: Departments must implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored. At a minimum, ePHI on electronic media must be disposed of through: clearing (using software or hardware products to format or overwrite media in order to render ePHI indecipherable or inaccessible); purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains); or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

2. Media Re-Use: Departments must implement procedures for the removal of ePHI from electronic media before the media are made available for re-use. Prior to making storage devices and removable media available for reuse, workforce members must ensure that the device or media does not contain ePHI.

3. Accountability: Departments are required to maintain a record of the movements of hardware and electronic media. Departments must designate a person responsible for tracking the movements of hardware and electronic media containing ePHI within the department.

4. Data Backup and Storage: A retrievable, exact copy of ePHI, must be created when needed, before movement of equipment.

D. Paper Document Controls

Departments must implement policies and procedures to secure and protect paper documents containing PHI. Policies and procedures must address at a minimum, the following:

1. Storage of PHI*:* PHI in paper records must be secured at all times. PHI must be stored in a locked desk, filing cabinet, office or storage/file room. Keys for access to filing cabinets, desks, offices and storage/file rooms must not be left unattended on a desk or stored in a manner that is accessible to unauthorized persons. Individual shred boxes must be disposed of when leaving your work area.

2. Clean Desk Policy*:* Workforce members shall ensure that all PHI in paper and electronic form is secured in the work area when leaving the area for any amount of time and at the end of the day. All PHI must be removed from the desk and locked in a secure location, e.g. locked

drawer, file cabinet, or file room, unless located in a locked office or other approved secure area.

3. Printers and Faxes*:* Fax machines and printers must be kept in secured areas where information is not available to unauthorized workforce members or the public. Workforce members must verify the fax number with the intended recipient prior to sending PHI via fax. Fax machines and printers must be cleared regularly to ensure PHI remains protected and secured.

4. Mail*:* A secure courier with signature receipt must be utilized when sending large volumes of PHI. In addition, disks and other transportable media sent through mail or courier must be encrypted prior to sending.

5. Safeguarding PHI*:* PHI shall not be left unattended on desks or in unsecured areas, including conference rooms or public access areas. When traveling with PHI, PHI must not be left unattended or unsecured in checked baggage or in a public location. PHI should not be left unattended in a vehicle, however if necessary PHI may be secured in the trunk of a vehicle. PHI must not be left unattended in a vehicle overnight.

6. Destruction of PHI*:* PHI in paper form shall be disposed of by shredding the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed. Hard copies that contain PHI must be disposed of in containers designated for storage of such documents prior to destruction, e.g. shred bins. PHI deposited in a shred bin must be fully encompassed in the shred bin to prevent removal, and the shred bin must not be overfilled.

Technical Safeguards

A. Access Control: Departments shall implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R. §164.308(a)(4). The policies and procedures shall at a minimum require the following:

1. Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.

2. Emergency Access Procedure: Establish procedures for obtaining necessary ePHI during an emergency.

3. Automatic logoff: Computer systems containing ePHI must be set to automatically log off after no more than 10 minutes of inactivity. Workforce members shall lock or log off a system containing ePHI whenever leaving the system unattended.

4. Encryption and Decryption: Implement a mechanism to encrypt and decrypt ePHI.

5. Password Management: Access to any workstation, program, process or system that contains ePHI shall be protected through the use of a unique User ID and password. Passwords shall not be common or easily identifiable (birthday, name, etc.). Passwords should not include dictionary words. Employees shall not share or make accessible User IDs or passwords. Passwords shall be changed no less than every 90 days. Departments must implement a lockout process after a specified number of failed attempts to access a workstation or system.

B. Audit Controls: Departments shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Departments shall implement procedures for monitoring log-in attempts and reporting discrepancies.

C. Integrity: Departments shall implement policies and procedures to protect ePHI from improper alteration or destruction.

1. Mechanism to Authenticate ePHI: Departments shall implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

2. Protection from Malicious Software: Departments shall implement procedures for guarding against, detecting, and reporting malicious software.

D. Transmission Security: Departments shall implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

1. Encryption Safeguards
   Departments shall use appropriate encryption to protect ePHI stored on portable devices or transmitted across an unsecured network such as the internet or wireless network in accordance with HIPAA regulations. Departments shall implement written policies and procedures for encrypting and decrypting ePHI as appropriate.

   a. *Encryption Standard*: ePHI must be secured using a Federal Information Processing Standard (FIPS) approved algorithm. In accordance with National Institute for Standards and Technology (NIST), whenever possible, Advanced Encryption Standard (AES) should be used for the encryption algorithm based on its strength and speed.

   b. *Email*: Email containing ePHI must be encrypted prior to sending outside of the County network.

   c. *Desktops, Laptops and Tablet Computers*: All County-owned desktops, laptops and tablet computers used to store ePHI must utilize Full Disk Encryption (FDE). Staff shall not store ePHI on personally owned devices.

   d. *Mobile Devices*: Departments must have policies, procedures and safeguards in place that address the use and security of County-owned and personal mobile devices. Mobile devices include, but are not limited to, smart phones, blackberries, phablets, personal digital assistants (PDAs) and smart watches.

   e. *Universal Serial Bus (USB) Drives, External Hard Drives, CDs and DVDs*: USB drives (also known as thumb drives, jump drives, flash drives), external hard drives, CDs and DVDs shall not be used to store ePHI unless the device or media is encrypted. The ePHI must be deleted or the device securely destroyed as soon as the ePHI is no longer required to be stored on the device or media.

   f. *Back-up Tapes:* Backup tapes used to store ePHI from servers must be encrypted. A secure accountability process must be implemented to store the tapes securely whether on or off site to prevent theft or loss of the tapes.

   g. *Remote Access:* All remote access into the department's network and systems must utilize an encryption mechanism to secure the connection and data from unauthorized access. Departments shall use standards such as a secure socket layer (SSL), Virtual Private Networking (VPN) or other equivalent alternative technology.

   h. *Wireless Networks*: Wireless networks used to transmit ePHI shall be secured using strong encryption standards. Wireless Equivalent Privacy (WEP) shall not be used as the encryption standard. Wireless networks used for guest or public access are exempt from

this requirement if the network is segregated from secure wireless networks in order to prevent unauthorized access.

2. *Emails*: Departments shall adopt policies and procedures to protect PHI when transmitted via email. The following minimum requirements must be addressed:

   a. Departments must ensure an automated confidentiality notice appears on all emails.

   b. PHI must never be included in the subject line of an email and only the minimum amount necessary may be included in the body of an email.

   c. PHI sent outside the County network must be encrypted through a solution approved by the Information Services Department (ISD).

   d. Prior to sending PHI via email, the sender must verify the recipient's email address.

Retention: Documentation required for compliance with this SP shall be retained for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

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

	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 04** **PAGE** 1 **OF** 2 **EFFECTIVE DATE** June 10, 2016
POLICY: HIPAA Policy **SP: Workforce Training**		**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

To ensure that all workforce members within the Health Care Component (HCC) receive training in accordance with the Health Insurance Portability and Accountability Act (HIPAA) which requires that covered entities train their workforce regarding privacy, security, policies, and procedures as necessary and appropriate for workforce members to carry out their functions (45 C.F.R. sections 164.530(b)(1) and 164.308(a)(5)).

DEPARTMENTS AFFECTED

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

DEFINITIONS

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.

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)

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).

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. Training shall be mandatory for all workforce members within the HCC, including management.

B. Verification of training must be documented and records must be retained for a minimum of six (6) years.

C. Training shall occur prior to accessing PHI upon initial employment, transfer, or promotion; and in no case later than 30 days from the date appointed to a HIPAA covered department.

D. Training shall include privacy, security, policies, and procedures such as:

   1. Uses and disclosures of PHI

   2. Complaint process

   3. Identifying and reporting breaches

   4. Administrative, physical and technical safeguards

5. Best practices

6. Fines and penalties

7. Other HIPAA concepts as appropriate

E. Staff should be retrained periodically, but at a minimum every two years.

F. Staff must be retrained upon a significant change in policy.

A County approved HIPAA training module is available through Performance Education Resource Center's (PERC) learning management system. Contact the Human Resources, Office of Compliance and Ethics for guidance.

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

	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 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

	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 06** **PAGE** 1 **OF** 7 **EFFECTIVE DATE** June 10, 2016
POLICY: HIPAA POLICY **SP: Uses and Disclosures of PHI**		**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

To establish standards regarding the use and disclosure of Protected Health Information (PHI).

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 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 (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)

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 Covered Entity in its role as employer).

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

Departments within the Health Care Component (HCC) must comply with the use and disclosure restrictions detailed below. PHI shall not be used or disclosed except as permitted by law.

A. **Disclosures within the County.** The following restrictions must be complied with by departments within the HCC and those departments receiving information from an HCC department.

1. Departments within the HCC cannot disclose PHI to a non-HCC department of the County without appropriate authorization or as permitted by the Privacy Rule.

2. Non-HCC departments that create or receive PHI from an HCC department shall only use or disclose that information in a manner consistent with the HIPAA regulations.

3. If employees perform duties for both an HCC and non-HCC department, they shall only use or disclose PHI created or received in the course of their work with the HCC in a manner consistent with the HIPAA regulations.

B. **Permitted Uses and Disclosures.** Generally PHI may be disclosed as follows:

1. To the individual;

2. For treatment, payment, or health care operations, as permitted by, and in compliance with the Privacy Rule and other applicable laws or regulations;

3. Incident to a use or disclosure otherwise permitted or required by the Privacy Rule, provided that the HCC has complied with the applicable requirements of the law with respect to such permitted or required uses or disclosures;

4. Except where prohibited under 45 C.F.R. §164.502(a)(5)(i), pursuant to and in compliance with a valid authorization;

5. Pursuant to an agreement under, or as otherwise permitted by, 45 C.F.R. §164.510;

6. As otherwise permitted by, and in compliance with, the applicable provisions of the Privacy Rule.

C. **Required Disclosures.** An HCC department is required to disclose PHI:

1. To an individual when requested under, and required by the Privacy Rule;

2. When required by the Secretary of Health and Human Services to investigate or determine the covered entity's compliance with the law; or

3. When otherwise required by law.

D. **Prohibited Uses and Disclosures.** HCC departments are prohibited from disclosing PHI as follows:

1. Using or disclosing PHI that is genetic information for underwriting purposes.

2. Selling PHI.

3. Using or disclosing PHI for marketing purposes, except pursuant to, and in compliance with, 45 C.F.R. §164.508(a)(3). HCC departments proposing to use or disclose PHI for marketing purposes shall consult with the County HIPAA Privacy Officer or the HCC department's privacy officer prior to undertaking such activities to ensure compliance with the law regarding specific authorization requirements for the purpose of marketing.

4. An HCC department that has agreed to a restriction pursuant to 45 C.F.R. §164.522(a)(1) may not use or disclose the PHI covered by the restriction in violation of such restriction, except as otherwise provided in 45 C.F.R. §164.522(a).

E. **Minimum Necessary Requirement.** When using or disclosing PHI or when requesting PHI from another covered entity or business associate, HCC departments must make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

1. Minimum necessary does not apply to:

   a. Disclosures to, or requests by, a health care provider for treatment;

   b. Uses or disclosures made to the individual, or the Secretary of Health and Human Services, as required by law;

   c. Uses or disclosures made pursuant to a valid authorization; or

   d. Uses and disclosures required by law.

2. For any type of disclosure that an HCC department makes on a routine and recurring basis, the HCC department must implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, the HCC department must develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and review requests for disclosure on an individual basis in accordance with such criteria.

3. An HCC department must limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made when requesting such information from other covered entities. For all uses, disclosures or requests to which this section applies, an HCC department may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

F. Limited Data Set

An HCC department may use or disclose a limited data set that meets the requirements of the Privacy Rule if the use of the limited data set is solely for the purpose of research, public health activities or health care operations. To utilize a limited data set, an HCC department must enter into a data use agreement with the limited data set recipient pursuant to the requirements of HIPAA.

HCC departments seeking to utilize a limited data set shall work with the HCC department privacy officer to ensure compliance with HIPAA requirements prior to disclosing information in a limited data set.

G. Uses and Disclosures Consistent with Notices of Privacy Practices

An HCC department that is required by the Privacy Rule to have a Notice of Privacy Practices may not use or disclose PHI in a manner inconsistent with such notice.

An HCC department that is required by the Privacy Rule to include a specific statement in its notice if it intends to engage in the noticed activity, must not use or disclose PHI for such activities unless the required statement is included in its notice.

H. Disclosures and Business Associates

A business associate (including internal business associates) may use or disclose PHI only as permitted or required by its business associate contract (or other permitted agreement pursuant to 45 C.F.R. §164.504(e)), or as required by law. The business associate may not use or disclose PHI in a manner that would violate the requirements of HIPAA if done by the covered entity, except for purposes specified in law, if such uses or disclosures are permitted by its contract or other arrangement. A business associate is required to disclose PHI: (1) when required by the Secretary of Health and Human Services to investigate or determine the business associate's compliance with the law; and (2) to the covered entity, individual or individual's designee, as necessary to satisfy a covered entities' obligations at law regarding an individual's request for PHI.

I. Disclosures by Whistleblowers and Victims of Crimes

An HCC department is not considered to have violated the requirements of the Privacy Rule if a member of its workforce or a business associate discloses PHI as a whistleblower provided that: (1) the workforce member or business associate (including an internal business associate) believes in good faith that the County has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by the County potentially endangers one or more patients, workers, or the public; and (2) the disclosure is to: (i) a health care oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions, or to an appropriate health care accreditation organization; or (ii) an attorney retained by or on behalf of the workforce member or business associate for the purpose of determining legal options.

An HCC department is not considered to have violated the requirements of the Privacy Rule if a member of its workforce who is a victim of a criminal act discloses PHI to a law enforcement official, provided that: (1) the PHI disclosed is about the suspected perpetrator of the criminal act; and (2) the PHI disclosed is limited to the information listed in 45 C.F.R. §164.512(f)(2)(i).

J. Additional Federal or State Law Requirements

HIPAA establishes the minimum requirements for PHI uses and disclosures. HCC department records may be subject to additional Federal, State or contractual requirements regarding uses and disclosures that may prevent uses and disclosures otherwise permitted by HIPAA. HCC departments must follow all applicable requirements regarding uses and disclosures of PHI. Conflicts that arise in meeting all requirements will be submitted to the HCC department's privacy officer for review, and to County Counsel to resolve, if necessary.

K. Authorizations

Except as otherwise permitted or required by law, a covered entity may not use or disclose PHI without a valid authorization. When an HCC department obtains or receives a valid authorization for the use or disclosure of PHI, such use or disclosure must be consistent with that authorization. An HCC department must document and retain any signed authorization as

required by law, but for no less than six (6) years from the date of its creation, or the date when it last was in effect, whichever is later. If an HCC department seeks an authorization from an individual for a use or disclosure of PHI, the HCC department must provide the individual with a copy of the signed authorization.

PHI may be disclosed pursuant to a valid, signed authorization that meets the requirements of this Standard Practice, the provisions of 45 C.F.R. §164.508, and any other applicable State or Federal law. Generally, a valid authorization may contain elements or information in addition to the elements required by law, provided that such additional elements or information are not inconsistent with the elements required by law.

1. Valid Authorizations - A valid authorization must contain at least the following elements:

    a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

    b. The name or other specific identification of the person(s) or class of persons, authorized to make the requested use or disclosure;

    c. The name or other specific identification of the person(s) or class of persons, to whom the HCC department may make the requested use or disclosure;

    d. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;

    e. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of research study", "none", or similar language is sufficient if the authorization is for a use or disclosure of PHI for research;

    f. The signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided;

    g. Required statements - in addition to the above requirements, the authorization must contain the following statements adequate to put the individual on notice of all of the following:

        i. The individual's right to revoke the authorization in writing, and either:

            1. the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

            2. to the extent that the information on exceptions to the right to revoke and how to revoke the authorization are included in the Notice of Privacy Practices, a reference to the Notice;

        ii. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

            1. The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the

authorization when the prohibition on conditioning of authorization permitted by law applies; or

2. The consequences to the individual of a refusal to sign the authorization when the covered entity can, by law, condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization;

iii. The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by the applicable law;

h. The authorization must be written in plain language.

2. Defective Authorizations - An authorization is not valid if the document submitted has any of the following defects:

   a. The expiration date has passed or the expiration event is known by the HCC department to have occurred;

   b. The authorization has not been filled out completely, with respect to a required element, if applicable;

   c. The authorization is known by the HCC department to have been revoked;

   d. The authorization is an unpermitted compound authorization;

   e. Any material information in the authorization is known by the HCC to be false.

3. Compound Authorizations - An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization except as permitted by law. HCC departments wishing to use compound authorizations shall get the proposed authorization reviewed and approved by the HCC department privacy officer prior to use.

4. Prohibition on Conditioning of Authorizations - Generally an HCC department may not condition the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an authorization except as permitted by law. Exceptions are permitted for research-based treatment, eligibility, underwriting and risk determinations, or when health care is created solely for the purpose of disclosure to a third party.

5. Revocation of Authorization - An individual may revoke an authorization provided to an HCC department at any time, provided that the revocation is in writing, and except to the extent that: 1) the HCC department has taken action in reliance thereon; or 2) if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

6. Authorization Required - An HCC must obtain a valid authorization for the following specific uses or disclosures:

   a. Psychotherapy notes (as defined in 45 C.F.R. §164.501.)

   b. Marketing

c. Sale of PHI

If an HCC department wishes to use or disclose PHI or conduct the activities listed above, the HCC department privacy officer must be consulted prior to the use or disclosure.

HCC departments are responsible for creating a standardized authorization form to be used within the HCC department. HCC departments may have additional legal requirements relating to the form and substance of an authorization for their specific records and shall address those additional requirements in the standardized authorization form. Questions of sufficiency of any authorization are to be determined by either the HCC department privacy officer or County Counsel.

In the event that an HCC department receives more than one authorization or permission from an individual, and the authorizations appear to be in conflict with each other, the HCC department will abide by the more restrictive authorization until the conflict is resolved with the individual who is the subject of the authorization.

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

	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 07** **PAGE** 1 **OF** 8 **EFFECTIVE DATE** June 10, 2016
POLICY: HIPAA POLICY **SP: Patient Privacy Rights**		**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

To establish standards regarding the privacy rights of patients.

DEPARTMENTS AFFECTED

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

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

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)

Health Oversight Agency: An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility in compliance, or to enforce civil rights laws for which health information is relevant.

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.

Notice of Privacy Practices: A notification provided to patients that describes how their information may be used or shared and how they can exercise their patient privacy rights.

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 Covered Entity in its role as employer).

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. HIPAA provides an individual with certain privacy rights regarding their PHI. Health Care Component (HCC) departments shall have policies and procedures that address those rights and establish methods by which an individual may exercise those rights. At a minimum HCC departments shall have policies and procedures that address a patient's right to:

1. Receive a copy of the Notice of Privacy Practices and a method for obtaining an acknowledgement of receipt for that Notice;

2. Access their PHI;

3. Request an amendment of their PHI;

4. An Accounting of Disclosures of their PHI;

5. Request special restrictions on the use or disclosure of their PHI; and

6. Request a restriction on, or special directions regarding, the manner and method of communicating PHI.

B. Notice of Privacy Practices

An individual has a right to receive notification regarding the HCC department's privacy practices so the individual can understand how their PHI will be used and disclosed by the HCC department. The County has developed a template Notice of Privacy Practices containing the minimum legal requirements to guide HCC departments in developing the content for their Notice of Privacy Practices. The template Notice of Privacy Practices is available on the Human Resources Office of Compliance and Ethics website.

The template Notice may be customized to reflect the privacy practices of the HCC department, but the HCC department shall adhere to the minimum legal requirements for its line of business. Once distributed, the HCC department shall adhere to the practices contained in the Notice until it has been revised and re-published as required by law.

1. HCC departments with a direct treatment relationship shall:

   a. Provide the notice to the individual no later than the date of first service delivery. If the first service delivery is provided electronically, the HCC department must send the notice electronically, automatically and contemporaneously with the first service delivery. In an emergency treatment situation, the notice must be provided as soon as reasonably practicable;

   b. Make the notice available for individuals to take with them;

c. Post the notice in a clear and prominent location where it is reasonable to expect patients to be able to read the notice;

d. Post the notice prominently on any website that it maintains containing information about the department's services and make the notice available electronically through the website; and

e. Upon revision, make the revised notice available upon request and post the revised notice in the facility and on the website.

2. HCC departments that do not have a direct treatment relationship with individuals must make notices available to individuals only if they request one. HCC departments that are health plans must provide a Notice of Privacy Practices to their clients every three (3) years.

3. Except in the case of an emergency treatment situation, an HCC department must make a good faith effort to obtain a written acknowledgment that the individual received the Notice of Privacy Practices. If the individual refuses to sign or a signed acknowledgment is not obtained for some other reason, the HCC department shall document the good faith efforts taken and the reason why the acknowledgment was not obtained.

4. HCC departments must promptly revise their Notice whenever there has been a material change to the uses or disclosures, the individual's rights, the HCC department's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the Notice shall not be implemented prior to the effective date of the Notice in which the material change is reflected.

5. HCC departments must document compliance with the Notice and Acknowledgment requirements by retaining copies of these documents for a minimum of six (6) years.

C. Access to PHI

1. In general, individuals, or their personal representative (hereinafter collectively referred to as "individuals") may access, inspect, and receive a copy of the PHI that was created or received by an HCC department and is maintained in a designated record set, except as provided for by law.

2. Individuals requesting access to records must submit their request to the HCC department in writing. If the request indicates that the individual is seeking records from more than one County department, the request form shall be forwarded to the County HIPAA Privacy Officer for response. The County HIPAA Privacy Officer will coordinate the compilation of records from each department so that a single response is provided to the records request.

3. HCC departments must provide PHI in the form and format requested by the individual if it is readily producible in such form and format. If the requested form or format is not readily producible, HCC departments must give the individual a readable hard copy or provide the information in another mutually agreed upon format.

4. If an HCC component maintains PHI electronically and an individual requests access to ePHI, HCC departments must provide an electronic copy, but are not required to provide direct access to electronic records systems. Requests for electronic copies of records must be provided in the form or format requested if it is readily producible in such form or format. If it is not readily producible in the form or format requested, the HCC department must provide it in a machine-readable electronic form and format as agreed to by the HCC department and the individual. Machine readable electronic form or format means digital information stored in a standardized format enabling the information to be processed and analyzed by computer.

Examples include MS Word, Excel, plain text, HTML, text-based PDF, etc. If the individual declines to accept any of the formats that are readily producible by the HCC department, a hard copy may be provided to fulfill the request.

5. If an individual's request for access directs the HCC department to transmit the PHI directly to another person, the HCC department must provide the copy to the person designated on a valid authorization. The request must be in writing, signed by the individual, and clearly identify the designated person and where to send the information. ePHI delivered or transmitted outside the HCC department shall be encrypted utilizing the County or department encryption software. An exception can be made for circumstances where technological incompatibility prevents successful delivery or transmission of the information, or when the individual has requested the information not be encrypted. In those instances the HCC department will work with the receiving party to provide the most secure method of delivery or transmission possible. When an individual has requested the information not be transmitted in an encrypted form, the HCC department may send unencrypted PHI at their discretion, if the HCC department has advised the individual of the risks, and the individual still prefers the unencrypted Email.

6. Requests for access to or copies of PHI shall be completed by providing access to, or copies of, the applicable records, or portions of the records, requested to the individual.

7. HCC departments may only provide a summary of requested PHI, when an individual requests or agrees, in advance, to receiving a summary. If a summary is prepared, the following requirements must be met:

    a. Summary of the entire record unless the individual limits the request to a specific injury, illness, episode, hospitalization or timeframe.

    b. Relative to the a specific injury, illness, episode, hospitalization or timeframe, the summary must include:

        i. Chief complaint, including pertinent history

        ii. Findings from consultation and referrals to other health care providers

        iii. Diagnosis, where determined

        iv. Treatment plans, including any medications prescribed

        v. Progress of the treatment

        vi. Prognosis, including significant continuing problems or conditions

        vii. Pertinent reports of diagnostic procedures and all discharge summaries

        viii. Objective findings from the most recent physical examination, including blood pressure, weight and actual values from laboratory tests

    c. All current medications prescribed, including dosage, and any sensitivities or allergies to medications recorded by the provider.

8. Access to records for inspection by the individual must be provided within five (5) working days of receiving the written request. Copies must be provided within fifteen (15) days of receipt of request for copies.

9. An HCC department may only deny an individual access to PHI when permitted by law. If the HCC department denies the request, in whole or in part, it must provide the individual with a written denial as required by law. When an HCC department intends to deny access or copies of PHI to the individual, they should consult with the HCC department privacy officer prior to notifying the individual of the denial of access.

10. HCC departments shall have a policy that describes how an individual can request access to, and receive copies of, PHI in the designated record set, and which documents the titles of the persons or offices responsible for receiving and processing requests. HCC departments must maintain the associated documentation as required by law.

D. Requests for Amendment of PHI

1. An individual has the right to have an HCC department amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

2. HCC departments shall have a policy that describes how an individual can request an amendment to PHI in the designated record set, which documents the titles of the persons or offices responsible for receiving and processing requests for amendments, the process for actually amending the PHI and maintenance of the documentation as required by law. HCC departments shall act on the individual's request in a timely manner, and in no case later than 60 days after receipt of request.

3. An HCC department that has been notified by another covered entity of an amendment to an individual's PHI must amend the PHI in designated record sets as required by law.

4. An HCC may deny an individual's request for amendment if it determines that the PHI or record(s) that is the subject of the request:

    a. Was not created by the HCC department, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

    b. Is not part of the designated record set;

    c. Would not be information available to the individual's inspection under law; or

    d. Is accurate and complete.

E. Accounting of Disclosures of PHI

1. An individual has a right to receive an accounting of disclosures of PHI made by an HCC department.

2. The HCC department must provide the individual with a written accounting for the time requested, or for disclosures that occurred during the last six (6) years, including disclosures to or by business associates of the HCC department. The accounting must include:

    a. The date of the disclosure;

    b. The name of the entity or person who received the PHI and, if known, the address of such entity or person;

    c. A brief description of the PHI disclosed; and

d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under 45 C.F.R. §164.502(a)(2)(ii) or 164.512, if any.

3. HCC departments must account for the following disclosures of PHI when made without a HIPAA-compliant authorization from the patient, including but not limited to:

   a. In connection with judicial and administrative proceedings (for example, pursuant to a subpoena or court order)

   b. For public health activities and reporting

   c. To the Food and Drug Administration

   d. To report injuries by firearms, assaultive or abusive conduct

   e. About victims of abuse, neglect, domestic violence

   f. For health oversight activities (unless for treatment, payment or operations)

   g. To a law enforcement official

   h. To coroners, medical examiners, funeral directors

   i. For cadaveric organ, eye or tissue donation

   j. For certain specialized government functions

   k. For workers' compensation purposes

   l. To business associates (unless for treatment, payment or operations)

   m. To researchers

   n. To the Secretary of the U.S. Department of Health and Human Services

   o. To avert a serious threat to health or safety

   p. Disclosures required by law

   q. Unlawful and unauthorized disclosures outside the facility (breaches)

4. The following do not require an accounting of disclosures:

   a. To carry out treatment, payment and health care operations permitted by law;

   b. To the individual regarding their own PHI;

   c. Incident to a use or disclosure otherwise permitted or required by the Privacy Rule;

   d. Pursuant to a valid authorization;

   e. For a facility directory or to persons involved in the individual's care or other notification purposes as permitted by law;

f. For national security or intelligence purposes as provided in 45 C.F.R. §164.512(k)(2);

g. To correctional institutions or law enforcement officials as permitted or required by law;

h. As part of a limited data set in accordance with 45 C.F.R. §164.512(e); or

i. That occurred prior to the compliance date for the HCC department.

5. The first accounting to an individual in any 12 month period must be provided without charge. HCC departments shall have a policy which describes how an individual can request an accounting of disclosures of PHI as provided by the Privacy Rule and which documents the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

6. An accounting of disclosures is necessary for disclosures made for research purposes. HCC departments are not required to inform individuals each time PHI is disclosed for research purposes. If an accounting of disclosures is requested by an individual and the HCC department has made a disclosure for research purposes for 50 or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide a simplified accounting which includes the following:

   a. The name of the protocol of research activity

   b. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

   c. A brief description of the type of PHI that was disclosed;

   d. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

   e. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and,

   f. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

7. An HCC department may suspend or place a temporary hold on an individual's right to receive an accounting of disclosures when requested by a Health Oversight Agency or Law Enforcement Official.

   a. If the agency or official provides a written statement that specifies: (1) such an accounting to the individual would be reasonably likely to impede the agency's activities; and, (2) the time for which such a suspension is required, then the release of the accounting shall be suspended for the time specified by the agency or official.

   b. If the agency or official provides an oral statement that a suspension is necessary, the HCC department must: (1) document the statement including the identity of the individual making the statement and the agency or official on whose behalf the statement is made; (2) temporarily suspend the individual's right to an accounting subject to the statement; and, (3) limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement providing a time limit is submitted during the 30 days.

F. Requests for Special Restrictions on PHI

1. An HCC department must permit an individual to request that the covered entity restrict:

    a. Uses and disclosures of PHI about the individual to carry out treatment, payment or health care operations; and

    b. Information released to family or close friends involved in the patient's care or payment for that care, or to notify a family member of the patient's location.

2. An HCC department is not required to agree to a restriction except when an individual requests PHI not be disclosed to a health plan, if:

    a. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

    b. The PHI pertains solely to a health care item or service for which the individual or person other than the health plan on behalf of the individual, has paid the HCC department out of pocket in full.

3. An HCC department that agrees to a requested restriction of PHI may not use or disclose such PHI in violation of such restriction, except that if the individual who requested the restriction is in need of emergency treatment and the restricted information is needed to provide the emergency treatment, the HCC department may use the restricted information, or may disclose such information to a health care provider to provide such treatment to the individual. If restricted information is disclosed to a health care provider for emergency treatment, the HCC department must request that such health care provider not further use or disclose the information. A restriction agreed to by the HCC department is not effective to prevent uses or disclosures permitted or required under 45 C.F.R. §§164.502(a)(2)(ii), 164.510(a) or 164.512. HCC departments shall have a policy which describes how an individual can request a restriction on the use or disclosure of PHI and which also describes the process for terminating a restriction. An HCC department must document a restriction in accordance with 45 C.F.R. §164.530(j).

G. Request for Alternative Communication Methods

1. An HCC department must permit individuals to request, and must accommodate reasonable requests by individuals, to receive communications of PHI from the HCC department by alternative means or alternative locations. An HCC department may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

2. HCC departments shall have a policy which describes how an individual can request an alternative communication method and which describes any conditions on the provision of a reasonable accommodation, if applicable.

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

	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 08** **PAGE** 1 **OF** 4 **EFFECTIVE DATE** June 10, 2016
POLICY: HIPAA POLICY **SP: Business Associate Agreements**		**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

To establish guidelines regarding agreements between the County and Business Associates in accordance with the Health Insurance Portability and Accountability Act (HIPAA).

DEPARTMENTS AFFECTED

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

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

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.

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 Covered Entity in its role as employer).

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.)

PROCEDURES

A. Except as provided in paragraph D., business associate means, with respect to a covered entity, a person who:

1. On behalf of such covered entity, or an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by 45 C.F.R. Parts 160, 162 or 164, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. section 3.20, billing, benefit management, practice management and repricing; or

2. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the services involves the disclosure of PHI from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

B. A covered entity maybe a business associate of another covered entity.

C. Business associate includes:

1. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a covered entity and that requires access on a routine basis to such PHI.

2. A person that offers a personal health record to one or more individuals on behalf of a covered entity.

3. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

D. Business associate does not include:

1. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

2. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or Health Maintenance Organization with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 C.F.R. section 164.504(f) apply and are met.

3. A government agency with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.

4. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph A.1. of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph A.2. of this definition to or for such organized health care arrangement by virtue of such activities or services.

E. Health Care Component (HCC) departments shall consult with County Counsel to resolve questions with respect to business associate relationships.

F. An HCC department may allow a business associate to create, receive, maintain, or transmit PHI on the HCC department's behalf only if the HCC department obtains satisfactory assurances, that the business associate will appropriately safeguard the information in compliance with the provisions below. An HCC department is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

Written Contract or Other Arrangement: HCC departments must document the satisfactory assurances through a written contract or other arrangement with the business associate that meets the following requirements:

1. *Business Associate Contracts*: The contract must:

    a. Establish the permitted and required uses and disclosures of PHI by the business associate.

    b. Provide that the business associate will:

        i. Not use or further disclose the information other than as permitted or required by contract or law;

        ii. Use appropriate safeguards and comply, where applicable, with the HIPAA Security Rule with respect to ePHI, to prevent use or disclosure of the information other than as provided for by the contract;

        iii. Report to the HCC department any use or disclosure of the information not provided for by the contract of which it becomes aware, including breaches of unsecured PHI;

        iv. Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

        v. Make available PHI in accordance with 45 C.F.R. section 164.524;

        vi. Make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. section 164.526;

        vii. Make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. section 164.528;

        viii. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the department available to the Secretary of Health and Human Services for purposes of determining the HCC department's compliance with HIPAA; and

        ix. At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the HCC department that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

c. Authorize termination of the contract by the HCC department, if the HCC department determines that the business associate has violated a material term of the contract.

2. *Other Arrangements*: If the business associate is a governmental entity, the HCC department may comply with this requirement by entering into a memorandum of understanding with the business associate that contains the terms that meet the objectives listed above. Arrangements between an HCC department and an internal business associate must be documented in a memorandum of understanding that complies with this Standard Practice.

3. *Performance Required by Law:* If a business associate is required by law to perform a function or activity on behalf of the HCC department or to provide a service described in the definition of a business associate by 45 C.F.R. section 160.103 to an HCC department, the HCC department may disclose PHI to the business associate to the extent necessary to comply with the legal mandate without a contract, provided the HCC department attempts in good faith to obtain satisfactory assurances in accordance with section F.1. above.

4. *Limited Data Sets*: The HCC department may comply with these requirements if the HCC department discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the HCC department has a data use agreement with the business associate that complies with 45 C.F.R. sections 164.514(e)(4) and 164.314(a)(1), as applicable.

5. *Countywide Template*: A countywide business associate agreement template has been developed as a guideline for HCC departments and may be accessed on the Human Resources Office of Compliance and Ethics website.

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

	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 impermissible or unauthorized acquisition, 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 acquisition, access, use or disclosure 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 specified 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 notification 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

	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 10** **PAGE** 1 **OF** 2 **EFFECTIVE DATE** June 10, 2016
POLICY: HIPAA Policy **SP: HIPAA Complaint Process**		**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

This establishes the process for Health Insurance Portability and Accountability Act (HIPAA) complaints submitted to the County of San Bernardino.

DEPARTMENTS AFFECTED

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

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)

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

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).

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. **Filing of HIPAA Complaints**:

Any person or entity who believes that the County, any member of the County's workforce, or any County business associate, has violated or is otherwise not complying with the privacy and security requirements of HIPAA or this Standard Practice may submit a complaint.

Any such complaint may be submitted to any department supervisor, manager, or administrator, or to any County department privacy or security officer, or the County Privacy Officer. It is preferable that complaints be submitted in writing.

A complaint may also be filed with:

Office of Compliance and Ethics
157 W. 5th Street, 1st Floor,
San Bernardino, CA 92415-0440
Phone: 909-387- 4500 FAX: 909-387-8950
Email: hipaacomplaints@cao.sbcounty.gov
Website: https://www.integrity-helpline.com/SBC_C&E.jsp

or

Region IX
Office for Civil Rights
U.S. Department of Health and Human Services (DHHS)
90 7th Street, Suite 4-100
San Francisco, CA 94103
Phone: 800-368-1019 TTY: 800-537-7697
FAX: 415-437-8329
Website: https://www.hhs.gov/ocr/privacy/hipaa/complaints/

B. HIPAA Complaint Process

The County department, program, or person who receives the HIPAA related complaint shall follow a standardized and consistent process for review:

1. HIPAA complaints filed directly with the County Privacy Officer shall be copied to the individual County department.
2. HIPAA complaints filed through the online incident reporting site shall be copied to the County department and the County Privacy Officer.
3. The County Privacy Officer and the involved County department shall maintain collaborative dialogue and review of complaints.
4. HIPAA complaints shall be acknowledged in writing within five (5) business days of receipt.
5. Findings and recommendations, if any, shall be documented.
6. The individual County departments and the County Privacy Officer shall each maintain a log of complaints received including, but not limited to, dates of complaint, name of complainant, date of referral, referral contact and follow-up/response.
7. HIPAA complaints filed with the individual County departments and any subsequent documentation shall be maintained on file and provided to the County Privacy Officer upon request.

C. No Retaliation

No person shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or organization that exercises any rights granted by HIPAA, including, but not limited to, filing a complaint or assisting in the lawful investigation of such a complaint, or opposing any act or practice made unlawful by HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful or violates HIPAA, and the manner of the opposition is reasonable and does not involve an improper disclosure of protected health information in violation of HIPAA.

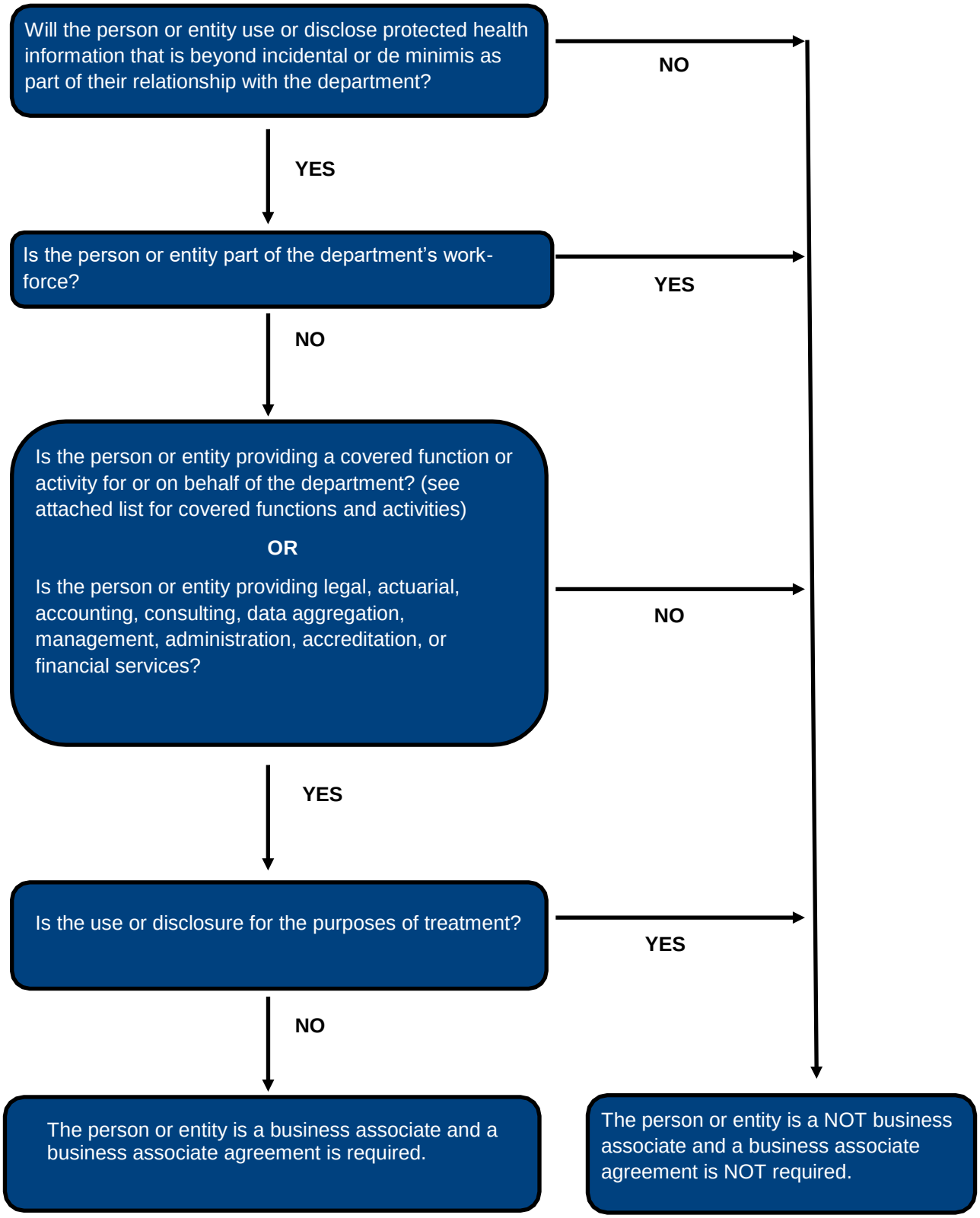
D. Office for Civil Rights (OCR)

If a County department is contacted by the OCR regarding a complaint made directly to OCR, the department shall cooperate with the OCR's investigation and immediately notify the County Privacy Officer.

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 Standard Practice to the particular needs of their departments.

LEAD DEPARTMENT
Human Resources

APPENDIX C
BUSINESS ASSOCIATE FLOW CHART



Business associate functions and activities include:

- Claims processing or administration
- Data analysis, processing or administration
- Utilization review
- Quality assurance
- Billing
- Benefit management
- Practice management
- Repricing

Exceptions to the definition of a business associate include:

- Disclosures by a covered entity to another health care provider for treatment of a patient.
- Disclosures to a health plan by a health care provider for purposes of payment.
- Relationships with persons or entities whose functions or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all. For example, janitorial or building maintenance contracts.
- With a person or entity that acts merely as a conduit for PHI. For example, the US postal service.
- A government agency that determines eligibility for or enrollment in a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes.

When in doubt, contact your County Counsel to discuss whether a relationship requires a business associate agreement.

APPENDIX D
BUSINESS ASSOCIATE AGREEMENT TEMPLATES

BUSINESS ASSOCIATE AGREEMENT
[Exhibit Version]

This Business Associate Agreement (Agreement) supplements and is made a part of the contract (Contract) by and between the County of San Bernardino [DEPARTMENT] (hereinafter Covered Entity) and [INSERT CONTRACTOR NAME HERE] (hereinafter Business Associate). This Agreement is effective as of the effective date of the Contract.

RECITALS

WHEREAS, Covered Entity (CE) wishes to disclose certain information to Business Associate (BA) pursuant to the terms of the Contract, which may include Protected Health Information (PHI); and

WHEREAS, CE and BA intend to protect the privacy and provide for the security of the PHI disclosed to BA pursuant to the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (HITECH Act), their implementing regulations, and other applicable laws; and

WHEREAS, The Privacy Rule and the Security Rule require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, sections 164.314, subdivision (a), 164.502, subdivision (e), and 164.504, subdivision (e) of the Code of Federal Regulations (C.F.R.) and contained in this Agreement; and

WHEREAS, Pursuant to HIPAA and the HITECH Act, BA shall fulfill the responsibilities of this Agreement by being in compliance with the applicable provisions of the HIPAA Standards for Privacy of PHI set forth at 45 C.F.R. sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards), 164.316 (Policies and Procedures and Documentation Requirements), and, 164.400, et seq. and 42 United States Code (U.S.C.) section 17932 (Breach Notification Rule), in the same manner as they apply to a CE under HIPAA;

NOW THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

A. Definitions

Unless otherwise specified herein, capitalized terms used in this Agreement shall have the same meanings as given in the Privacy Rule, the Security Rule, the Breach Notification Rule, and HITECH Act, as and when amended from time to time.

1. Breach shall have the same meaning given to such term under the HIPAA Regulations [45 C.F.R. §164.402] and the HITECH Act [42 U.S.C. §§17921 et seq.], and as further described in California Civil Code section 1798.82.
2. Business Associate (BA) shall have the same meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to 42 U.S.C. section 17921 and 45 C.F.R. section 160.103.
3. Covered Entity (CE) shall have the same meaning given to such term as under the Privacy Rule and Security Rule, including, but not limited to 45 C.F.R. section 160.103.

4. Designated Record Set shall have the same meaning given to such term under 45 C.F.R. section 164.501.
5. Electronic Protected Health Information (ePHI) means PHI that is maintained in or transmitted by electronic media as defined in the Security Rule, 45 C.F.R. section 164.103.
6. Individual shall have the same meaning given to such term under 45 C.F.R. section 160.103.
7. Privacy Rule means the regulations promulgated under HIPAA by the United States Department of Health and Human Services (HHS) to protect the privacy of Protected Health Information, including, but not limited to, 45 C.F.R. Parts 160 and 164, subparts A and E.
8. Protected Health Information (PHI) shall have the same meaning given to such term under 45 C.F.R. section 160.103, limited to the information received from, or created or received by Business Associate from or on behalf of, CE.
9. Security Rule means the regulations promulgated under HIPAA by HHS to protect the security of ePHI, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, subparts A and C.
10. Unsecured PHI shall have the same meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act, including, but not limited to 42 U.S.C. section 17932, subdivision (h).

B. Obligations and Activities of BA

1. Permitted Uses and Disclosures

   BA may disclose PHI: (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) for purposes of Treatment, Payment and Operations (TPO); (iv) as required by law; or (v) for Data Aggregation purposes for the Health Care Operations of CE. Prior to making any other disclosures, BA must obtain a written authorization from the Individual.

   If BA discloses PHI to a third party, BA must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such PHI will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify BA of any breaches of confidentiality of the PHI, to the extent it has obtained knowledge of such breach. [42 U.S.C. section 17932; 45 C.F.R. sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)]

2. Prohibited Uses and Disclosures

   i. BA shall not use, access or further disclose PHI other than as permitted or required by this Agreement and as specified in the attached Contract or as required by law. Further, BA shall not use PHI in any manner that would constitute a violation of the Privacy Rule or the HITECH Act. BA shall disclose to its employees, subcontractors, agents, or other third parties, and request from CE, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder.

   ii. BA shall not use or disclose PHI for fundraising or marketing purposes.

iii. BA shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates. (42 U.S.C. section 17935(a) and 45 C.F.R. section 164.522(a)(1)(i)(A).)

iv. BA shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CE and as permitted by the HITECH Act (42 U.S.C. section 17935(d)(2); and 45 C.F.R. section 164.508); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to this Agreement.

3. Appropriate Safeguards

i. BA shall implement appropriate safeguards to prevent the unauthorized use or disclosure of PHI, including, but not limited to, administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of the PHI BA creates, receives, maintains, or transmits on behalf of the CE, in accordance with 45 C.F.R. sections 164.308, 164.310, 164.312 and 164.316. [45 C.F.R. sections 164.504(e)(2)(ii)(b) and 164.308(b).]

ii. In accordance with 45 C.F.R. section 164.316, BA shall maintain reasonable and appropriate written policies and procedures for its privacy and security program in order to comply with the standards, implementation specifications, or any other requirements of the Privacy Rule and applicable provisions of the Security Rule.

iii. BA shall provide appropriate training for its workforce on the requirements of the Privacy Rule and Security Rule as those regulations affect the proper handling, use confidentiality and disclosure of the CE's PHI.

Such training will include specific guidance relating to sanctions against workforce members who fail to comply with privacy and security policies and procedures and the obligations of the BA under this Agreement.

4. Subcontractors

BA shall enter into written agreements with agents and subcontractors to whom BA provides CE's PHI that impose the same restrictions and conditions on such agents and subcontractors that apply to BA with respect to such PHI, and that require compliance with all appropriate safeguards as found in this Agreement.

5. Reporting of Improper Access, Use or Disclosure or Breach

Every suspected and actual Breach shall be reported immediately, but no later than one (1) business day upon discovery, to CE's Office of Compliance, consistent with the regulations under HITECH Act. Upon discovery of a Breach or suspected Breach, BA shall complete the following actions:

i. Provide CE's Office of Compliance with the following information to include but not limited to:

a) Date the Breach or suspected Breach occurred;

b) Date the Breach or suspected Breach was discovered;

c) Number of staff, employees, subcontractors, agents or other third parties and the names and titles of each person allegedly involved;

d) Number of potentially affected Individual(s) with contact information; and

e) Description of how the Breach or suspected Breach allegedly occurred.

i. Conduct and document a risk assessment by investigating without unreasonable delay and in no case later than five (5) calendar days of discovery of the Breach or suspected Breach to determine the following:

a) The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;

b) The unauthorized person who had access to the PHI;

c) Whether the PHI was actually acquired or viewed; and

d) The extent to which the risk to PHI has been mitigated.

ii. Provide a completed risk assessment and investigation documentation to CE's Office of Compliance within ten (10) calendar days of discovery of the Breach or suspected Breach with a determination as to whether a Breach has occurred. At the discretion of CE, additional information may be requested.

a) If BA and CE agree that a Breach has not occurred, notification to Individual(s) is not required.

b) If a Breach has occurred, notification to the Individual(s) is required and BA must provide CE with affected Individual(s) name and contact information so that CE can provide notification.

iv. Make available to CE and governing State and Federal agencies in a time and manner designated by CE or governing State and Federal agencies, any policies, procedures, internal practices and records relating to a Breach or suspected Breach for the purposes of audit or should the CE reserve the right to conduct its own investigation and analysis.

6. Access to PHI

To the extent BA maintains a Designated Record Set on behalf of CE, BA shall make PHI maintained by BA or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within ten (10) days of a request by CE to enable CE to fulfill its obligations under the Privacy Rule. If BA maintains ePHI, BA shall provide such information in electronic format to enable CE to fulfill its obligations under the HITECH Act. If BA receives a request from an Individual for access to PHI, BA shall immediately forward such request to CE.

7. Amendment of PHI

If BA maintains a Designated Record Set on behalf of the CE, BA shall make any amendment(s) to PHI in a Designated Record Set that the CE directs or agrees to, pursuant to 45 C.F.R. section 164.526, or take other measures as necessary to satisfy CE's obligations under 45 C.F.R. section 164.526, in the time and manner designated by the CE.

8. Access to Records

BA shall make internal practices, books, and records, including policies and procedures, relating to the use, access and disclosure of PHI received from, or created or received by BA on behalf of, CE available to the Secretary of HHS, in a time and manner designated by the Secretary, for purposes of the Secretary determining CE's compliance with the Privacy Rule and Security Rule and patient confidentiality regulations. Any documentation provided to the Secretary shall also be provided to the CE upon request.

9. Accounting for Disclosures

BA, its agents and subcontractors shall document disclosures of PHI and information related to such disclosures as required by HIPAA. This requirement does not apply to disclosures made for purposes of TPO. BA shall provide an accounting of disclosures to CE or an Individual, in the time and manner designated by the CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

10. Termination

CE may immediately terminate this agreement, and any related agreements, if CE determines that BA has breached a material term of this agreement. CE may, at its sole discretion, provide BA an opportunity to cure the breach or end the violation within the time specified by the CE.

11. Return of PHI

Upon termination of this Agreement, BA shall return all PHI required to be retained by the BA or its subcontractors, employees or agents on behalf of the CE. In the event the BA determines that returning the PHI is not feasible, the BA shall provide the CE with written notification of the conditions that make return not feasible. Additionally, the BA must follow established policies and procedures to ensure PHI is safeguarded and disposed of adequately in accordance with 45 C.F.R. section 164.310, and must submit to the CE a certification of destruction of PHI. For destruction of ePHI, the National Institute of Standards and Technology (NIST) guidelines must be followed. BA further agrees to extend any and all protections, limitations, and restrictions contained in this Agreement, to any PHI retained by BA or its subcontractors, employees or agents after the termination of this Agreement, and to limit any further use, access or disclosures.

12. Breach by the CE

Pursuant to 42 U.S.C. section 17934, subdivision (b), if the BA is aware of any activity or practice by the CE that constitutes a material Breach or violation of the CE's obligations under this Agreement, the BA must take reasonable steps to address the Breach and/or end eliminate the continued violation, if the BA has the capability of mitigating said violation. If the BA is unsuccessful in eliminating the violation and the CE continues with non- compliant activity, the BA must terminate the Agreement (if feasible) and report the violation to the Secretary of HHS.

13. Mitigation

BA shall have procedures in place to mitigate, to the extent practicable, any harmful effect that is known to BA of a use, access or disclosure of PHI by BA, its agents or subcontractors in violation of the requirements of this Agreement.

14. Costs Associated to Breach

BA shall be responsible for reasonable costs associated with a Breach. Costs shall be based upon the required notification type as deemed appropriate and necessary by the CE and shall not be reimbursable under the Agreement at any time. CE shall determine the method to invoice the BA for said costs. Costs shall incur at the current rates and may include, but are not limited to the following:

- Postage;
- Alternative means of notice;
- Media notification; and
- Credit monitoring services.

15. Direct Liability

BA may be held directly liable under HIPAA for impermissible uses and disclosures of PHI; failure to provide breach notification to CE; failure to provide access to a copy of ePHI to CE or individual; failure to disclose PHI to the Secretary of HHS when investigating BA's compliance with HIPAA; failure to provide an accounting of disclosures; and, failure to enter into a business associate agreement with subcontractors.

16. Indemnification

BA agrees to indemnify, defend and hold harmless CE and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages, penalties, injuries, costs and expenses (including costs for reasonable attorney fees) that are caused by or result from the acts or omissions of BA, its officers, employees, agents and subcontractors, with respect to the use, access, maintenance or disclosure of CE's PHI, including without limitation, any Breach of PHI or any expenses incurred by CE in providing required Breach notifications.

17. Judicial or Administrative Proceedings

CE may terminate the Contract, effective immediately, if (i) BA is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws or (ii) a finding or stipulation is made in any administrative or civil proceeding in which the BA has been joined that the BA has violated any standard or requirement of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws.

18. Insurance

In addition to any general and/or professional liability insurance coverage required of BA under the Contract for services, BA shall provide appropriate liability insurance coverage during the term of this Agreement to cover any and all claims, causes of action, and demands whatsoever made for loss, damage, or injury to any person arising from the breach of the security, privacy, or confidentiality obligations of BA, its agents or employees, under this Agreement and under HIPAA 45 C.F.R. Parts 160 and 164, Subparts A and E.

19. Assistance in Litigation or Administrative Proceedings

BA shall make itself, and any subcontractors, employees, or agents assisting BA in the performance of its obligations under the Agreement, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers, or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where BA or its subcontractor, employee or agent is a named adverse party.

C. Obligations of CE

1. CE shall notify BA of any of the following, to the extent that such may affect BA's use, access, maintenance or disclosure of PHI:
   i. Any limitation(s) in CE's notice of privacy practices in accordance with 45 C.F.R. section 164.520.
   ii. Any changes in, or revocation of, permission by an individual to use, access or disclose PHI.
   iii. Any restriction to the use, access or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. section 164.522.

D. General Provisions

1. Remedies

   BA agrees that CE shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which CE may have at law or in equity in the event of an unauthorized use, access or disclosure of PHI by BA or any agent or subcontractor of BA that received PHI from BA.

2. Ownership

   The PHI shall be and remain the property of the CE. BA agrees that it acquires no title or rights to the PHI.

3. Regulatory References

   A reference in this Agreement to a section in the Privacy Rule and Security Rule and patient confidentiality regulations means the section as in effect or as amended.

4. No Third-Party Beneficiaries

   Nothing express or implied in the Contract or this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CE, BA and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

5. Amendment

   The parties acknowledge that state and federal laws related to privacy and security of PHI are rapidly evolving and that amendment of the Contract or this Agreement may be required to ensure compliance with such developments. The parties shall negotiate in good faith to amend this Agreement when and as necessary to comply with applicable laws. If either party does not agree to so amend this Agreement within 30 days after receiving a request for amendment from the other, either party may terminate the Agreement upon written notice. To the extent an amendment to this Agreement is required by law and this Agreement has not been so amended to comply with the applicable law in a timely manner, the amendment required by law shall be deemed to be incorporated into this Agreement automatically and without further action required by either of the parties. Subject to the foregoing, this Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed and agreed to by BA and CE.

6. Interpretation

   Any ambiguity in this Agreement shall be resolved to permit CE to comply with the Privacy and Security Rules, the HITECH Act, and all applicable patient confidentiality regulations.

7. Compliance with State Law

   In addition to HIPAA and all applicable HIPAA Regulations, BA acknowledges that BA and CE may have confidentiality and privacy obligations under State law, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq. ("CMIA")). If any provisions of this Agreement or HIPAA Regulations or the HITECH Act conflict with CMIA or any other California State law regarding the degree of protection provided for PHI and patient medical records, then BA shall comply with the more restrictive requirements.

8. Survival

   The respective rights and obligations and rights of CE and BA relating to protecting the confidentiality or a patient's PHI shall survive the termination of the Contract or this Agreement.

BUSINESS ASSOCIATE AGREEMENT

[Stand Alone Agreement Version]

This Business Associate Agreement (Agreement) is entered into by and between the County of San Bernardino [DEPARTMENT] (hereinafter Covered Entity) and [INSERT CONTRACTOR NAME HERE] (hereinafter Business Associate).

RECITALS

WHEREAS, Covered Entity (CE) wishes to disclose certain information to Business Associate (BA) for the purposes of_____, which may include Protected Health Information (PHI); and

WHEREAS, CE and BA intend to protect the privacy and provide for the security of the PHI disclosed to BA pursuant to the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (HITECH Act), their implementing regulations, and other applicable laws; and

WHEREAS, The Privacy Rule and the Security Rule require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, sections 164.314, subdivision (a), 164.502, subdivision (e), and 164.504, subdivision (e) of the Code of Federal Regulations (C.F.R.) and contained in this Agreement; and

WHEREAS, Pursuant to HIPAA and the HITECH Act, BA shall fulfill the responsibilities of this Agreement by being in compliance with the applicable provisions of the HIPAA Standards for Privacy of PHI set forth at 45 C.F.R. sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards), 164.316 (Policies and Procedures and Documentation Requirements), and, 164.400, et seq. and 42 United States Code (U.S.C.) section 17932 (Breach Notification Rule), in the same manner as they apply to a CE under HIPAA;

NOW THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

A. Definitions

Unless otherwise specified herein, capitalized terms used in this Agreement shall have the same meanings as given in the Privacy Rule, the Security Rule, the Breach Notification Rule, and HITECH Act, as and when amended from time to time.

1. Breach shall have the same meaning given to such term under the HIPAA Regulations [45 C.F.R. §164.402] and the HITECH Act [42 U.S.C. §§17921 et seq.], and as further described in California Civil Code section 1798.82.
2. Business Associate (BA) shall have the same meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to 42 U.S.C. section 17921 and 45 C.F.R. section 160.103.
3. Covered Entity (CE) shall have the same meaning given to such term as under the Privacy Rule and Security Rule, including, but not limited to 45 C.F.R. section 160.103.
4. Designated Record Set shall have the same meaning given to such term under 45 C.F.R. section 164.501.
5. Electronic Protected Health Information (ePHI) means PHI that is maintained in or transmitted by electronic media as defined in the Security Rule, 45 C.F.R. section 164.103.
6. Individual shall have the same meaning given to such term under 45 C.F.R. section 160.103.

7. Privacy Rule means the regulations promulgated under HIPAA by the United States Department of Health and Human Services (HHS) to protect the privacy of PHI, including, but not limited to, 45 C.F.R. Parts 160 and 164, subparts A and E.

8. Protected Health Information (PHI) shall have the same meaning given to such term under 45 C.F.R. section 160.103, limited to the information received from, or created or received by Business Associate from or on behalf of, CE.

9. Security Rule means the regulations promulgated under HIPAA by HHS to protect the security of ePHI, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, subparts A and C.

10. Unsecured PHI shall have the same meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act, including, but not limited to 42 U.S.C. section 17932, subdivision (h).

B. Obligations and Activities of BA

1. Permitted Uses and Disclosures

   i. CE and BA shall exchange PHI for the following purposes: [set forth details as to purpose of the BAA and what information will be shared, and for what purpose.]

   ii. BA may disclose PHI (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) for purposes of Treatment, Payment and Operations (TPO); (iv) as required by law; or (v) for Data Aggregation purposes for the Health Care Operations of CE. Prior to making any other disclosures, BA must obtain a written authorization from the Individual.

   iii. If BA discloses PHI to a third party, BA must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such PHI will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify BA of any breaches of confidentiality of the PHI, to the extent it has obtained knowledge of such breach. [42 U.S.C. section 17932; 45 C.F.R. sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)]

2. Prohibited Uses and Disclosures

   i. BA shall not use, access or further disclose PHI other than as permitted or required by this Agreement or as required by law. Further, BA shall not use PHI in any manner that would constitute a violation of the Privacy Rule or the HITECH Act. BA shall disclose to its employees, subcontractors, agents, or other third parties, and request from CE, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder.

   ii. BA shall not use or disclose PHI for fundraising or marketing purposes.

   iii. BA shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates. (42 U.S.C. section 17935(a) and 45 C.F.R. section 164.522(a)(1)(i)(A).)

   iv. BA shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CE and as permitted by the HITECH Act (42 U.S.C. section 17935(d)(2); and 45 C.F.R. section 164.508); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to this Agreement.

3. Appropriate Safeguards

   i. BA shall implement appropriate safeguards to prevent the unauthorized use or disclosure of PHI, including, but not limited to, administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of the PHI BA creates, receives, maintains, or transmits on behalf of the CE, in accordance with 45 C.F.R. sections 164.308, 164.310, 164.312 and 164.316. [45 C.F.R. sections 164.504(e)(2)(ii)(b) and 164.308(b).]

   ii. In accordance with 45 C.F.R. section 164.316, BA shall maintain reasonable and appropriate written policies and procedures for its privacy and security program in order to comply with the standards, implementation specifications, or any other requirements of the Privacy Rule and applicable provisions of the Security Rule.

   iii. BA shall provide appropriate training for its workforce on the requirements of the Privacy Rule and Security Rule as those regulations affect the proper handling, use confidentiality and disclosure of the CE's PHI.

   The training will include specific guidance relating to sanctions against workforce members who fail to comply with privacy and security policies and procedures and the obligations of the BA under this Agreement.

4. Subcontractors

   BA shall enter into written agreements with agents and subcontractors to whom BA provides CE's PHI that impose the same restrictions and conditions on such agents and subcontractors that apply to BA with respect to such PHI, and that require compliance with all appropriate safeguards as found in this Agreement.

5. Reporting of Improper Access, Use or Disclosure or Breach

   Every suspected and actual Breach shall be reported immediately, but no later than one (1) business day upon discovery, to CE's Office of Compliance, consistent with the regulations under HITECH Act. Upon discovery of a Breach or suspected Breach, BA shall complete the following actions:

   i. Provide CE's Office of Compliance with the following information to include but not limited to:

      a) Date the Breach or suspected Breach occurred;

      b) Date the Breach or suspected Breach was discovered;

      c) Number of staff, employees, subcontractors, agents or other third parties and the names and titles of each person allegedly involved;

      d) Number of potentially affected Individual(s) with contact information; and

      e) Description of how the Breach or suspected Breach allegedly occurred.

   ii. Conduct and document a risk assessment by investigating without unreasonable delay and in no case later than five (5) calendar days of discovery of the Breach or suspected Breach to determine the following:

      a) The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;

      b) The unauthorized person who had access to the PHI;

      c) Whether the PHI was actually acquired or viewed; and

      d) The extent to which the risk to PHI has been mitigated.

iii. Provide a completed risk assessment and investigation documentation to CE's Office of Compliance within ten (10) calendar days of discovery of the Breach or suspected Breach with a determination as to whether a Breach has occurred. At the discretion of CE, additional information may be requested.

a) If BA and CE agree that a Breach has not occurred, notification to Individual(s) is not required.

b) If a Breach has occurred, notification to the Individual(s) is required and BA must provide CE with affected Individual(s) name and contact information so that CE can provide notification.

iv. Make available to CE and governing State and Federal agencies in a time and manner designated by CE or governing State and Federal agencies, any policies, procedures, internal practices and records relating to a Breach or suspected Breach for the purposes of audit or should the CE reserve the right to conduct its own investigation and analysis.

6. Access to PHI

To the extent BA maintains a Designated Record Set on behalf of CE, BA shall make PHI maintained by BA or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within ten (10) calendar days of a request by CE to enable CE to fulfill its obligations under the Privacy Rule. If BA maintains ePHI, BA shall provide such information in electronic format to enable CE to fulfill its obligations under the HITECH Act. If BA receives a request from an Individual for access to PHI, BA shall immediately forward such request to CE.

7. Amendment of PHI

If BA maintains a Designated Record Set on behalf of the CE, BA shall make any amendment(s) to PHI in a Designated Record Set that the CE directs or agrees to, pursuant to 45 C.F.R. section 164.526, or take other measures as necessary to satisfy CE's obligations under 45 C.F.R. section 164.526, in the time and manner designated by the CE.

8. Access to Records

BA shall make internal practices, books, and records, including policies and procedures, relating to the use, access and disclosure of PHI received from, or created or received by BA on behalf of, CE available to the Secretary of HHS, in a time and manner designated by the Secretary, for purposes of the Secretary determining CE's compliance with the Privacy Rule and Security Rule and patient confidentiality regulations. Any documentation provided to the Secretary shall also be provided to the CE upon request.

9. Accounting for Disclosures

BA, its agents and subcontractors shall document disclosures of PHI and information related to such disclosures as required by HIPAA. This requirement does not apply to disclosures made for purposes of TPO. BA shall provide an accounting of disclosures to CE or an Individual, in the time and manner designated by the CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

10. Termination

    CE may immediately terminate this agreement, and any related agreements, if CE determines that BA has breached a material term of this agreement. CE may, at its sole discretion, provide BA an opportunity to cure the breach or end the violation within the time specified by the CE.

11. Return of PHI

    Upon termination of this Agreement, BA shall return all PHI required to be retained by the BA or its subcontractors, employees or agents on behalf of the CE. In the event the BA determines that returning the PHI is not feasible, the BA shall provide the CE with written notification of the conditions that make return not feasible. Additionally, the BA must follow established policies and procedures to ensure PHI is safeguarded and disposed of adequately in accordance with 45 C.F.R. section 164.310, and must submit to the CE a certification of destruction of PHI. For destruction of ePHI, the National Institute of Standards and Technology (NIST) guidelines must be followed. BA further agrees to extend any and all protections, limitations, and restrictions contained in this Agreement, to any PHI retained by BA or its subcontractors, employees or agents after the termination of this Agreement, and to limit any further use, access or disclosures.

12. Breach by the CE

    Pursuant to 42 U.S.C. section 17934, subdivision (b), if the BA is aware of any activity or practice by the CE that constitutes a material Breach or violation of the CE's obligations under this Agreement, the BA must take reasonable steps to address the Breach and/or end eliminate the continued violation, if the BA has the capability of mitigating said violation. If the BA is unsuccessful in eliminating the violation and the CE continues with non-compliant activity, the BA must terminate the Agreement (if feasible) and report the violation to the Secretary of HHS.

13. Mitigation

    BA shall have procedures in place to mitigate, to the extent practicable, any harmful effect that is known to BA of a use, access or disclosure of PHI by BA, its agents or subcontractors in violation of the requirements of this Agreement.

14. Costs Associated to Breach

    BA shall be responsible for reasonable costs associated with a Breach. Costs shall be based upon the required notification type as deemed appropriate and necessary by the CE and shall not be reimbursable under the Agreement at any time. CE shall determine the method to invoice the BA for said costs. Costs shall incur at the current rates and may include, but are not limited to the following:

    - Postage;
    - Alternative means of notice;
    - Media notification; and
    - Credit monitoring services.

15. Direct Liability

    BA may be held directly liable under HIPAA for impermissible uses and disclosures of PHI; failure to provide breach notification to CE; failure to provide access to a copy of ePHI to CE or individual; failure to disclose PHI to the Secretary of HHS when investigating BA's compliance with HIPAA; failure to provide an accounting of disclosures; and, failure to enter into a business associate agreement with subcontractors.

16. Indemnification

BA agrees to indemnify, defend and hold harmless CE and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages, penalties, injuries, costs and expenses (including costs for reasonable attorney fees) that are caused by or result from the acts or omissions of BA, its officers, employees, agents and subcontractors, with respect to the use, access, maintenance or disclosure of CE's PHI, including without limitation, any Breach of PHI or any expenses incurred by CE in providing required Breach notifications.

17. Judicial or Administrative Proceedings

CE may terminate this Agreement, effective immediately, if (i) BA is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws or (ii) a finding or stipulation is made in any administrative or civil proceeding in which the BA has been joined that the BA has violated any standard or requirement of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws.

18. Insurance

BA shall provide appropriate liability insurance coverage during the term of this Agreement to cover any and all claims, causes of action, and demands whatsoever made for loss, damage, or injury to any person arising from the breach of the security, privacy, or confidentiality obligations of BA, its agents or employees, under this Agreement and under HIPAA 45 C.F.R. Parts 160 and 164, Subparts A and E.

19. Assistance in Litigation or Administrative Proceedings

BA shall make itself, and any subcontractors, employees, or agents assisting BA in the performance of its obligations under the Agreement, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers, or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where BA or its subcontractor, employee or agent is a named adverse party.

C. Obligations of CE

1. CE shall notify BA of any of the following, to the extent that such may affect BA's use, access, maintenance or disclosure of PHI:
   i. Any limitation(s) in CE's notice of privacy practices in accordance with 45 C.F.R. section 164.520.
   ii. Any changes in, or revocation of, permission by an individual to use, access or disclose PHI.
   iii. Any restriction to the use, access or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. section 164.522.

D. General Provisions

1. Term

This Agreement is effective as of _____ and shall continue for a period of _____ years/months unless otherwise terminated earlier by the Parties.

2. Remedies

BA agrees that CE shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which CE may have at law or in equity in the event of an unauthorized use, access or disclosure of PHI by BA or any agent or subcontractor of BA that received PHI from BA.

3. Ownership

   The PHI shall be and remain the property of the CE. BA agrees that it acquires no title or rights to the PHI.

4. Regulatory References

   A reference in this Agreement to a section in the Privacy Rule and Security Rule and patient confidentiality regulations means the section as in effect or as amended.

5. No Third-Party Beneficiaries

   Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CE, BA and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

6. Amendment

   The parties acknowledge that state and federal laws related to privacy and security of PHI are rapidly evolving and that amendment of this Agreement may be required to ensure compliance with such developments. The parties shall negotiate in good faith to amend this Agreement when and as necessary to comply with applicable laws. If either party does not agree to so amend this Agreement within 30 days after receiving a request for amendment from the other, either party may terminate the Agreement upon written notice. To the extent an amendment to this Agreement is required by law and this Agreement has not been so amended to comply with the applicable law in a timely manner, the amendment required by law shall be deemed to be incorporated into this Agreement automatically and without further action required by either of the parties. Subject to the foregoing, this Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed and agreed to by BA and CE.

7. Interpretation

   Any ambiguity in this Agreement shall be resolved to permit CE to comply with the Privacy Rule, Security Rule, the HITECH Act, and all applicable patient confidentiality regulations.

8. Compliance with State Law

   In addition to HIPAA and all applicable HIPAA Regulations, BA acknowledges that BA and CE may have confidentiality and privacy obligations under State law, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq. ("CMIA")). If any provisions of this Agreement or HIPAA Regulations or the HITECH Act conflict with CMIA or any other California State law regarding the degree of protection provided for PHI and patient medical records, then BA shall comply with the more restrictive requirements.

9. Survival

   The respective rights and obligations and rights of CE and BA relating to protecting the confidentiality or a patient's PHI shall survive the termination of this Agreement.

10. Choice of Law and Venue

    This Agreement shall be governed by and construed in all aspects in accordance with the laws of the State of California without regard to principles of conflicts of laws. The Parties agree to the exclusive jurisdiction of the federal court located in the County of Riverside and the state court located in the County of San Bernardino, for any and all disputes arising under this Agreement, to the exclusion of all other federal and state courts

IN WITNESS WHEREOF, the Covered Entity and Business Associate have each caused this Agreement to be subscribed by its respective duly authorized officers, on its behalf

BOARD OF SUPERVISORS

►

Robert A. Lovingood, Chairman, Board of Supervisors

Dated: _____

SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD

Laura H. Welch
Clerk of the Board of Supervisors
of the County of San Bernardino

By _____
Deputy

_____
(Print or type name of corporation, company, contractor, etc.)

By ► _____
(Authorized signature - sign in blue ink)

Name _____
(*Print or type name of person signing contract)*

Title _____
(Print or Type)

Dated: _____

Address _____

Approved as to Legal Form

►

_____
, County Counsel

Dated: _____

APPENDIX E
NOTICE OF PRIVACY PRACTICES TEMPLATE

SAN BERNARDINO COUNTY | XXX

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.
PLEASE REVIEW IT CAREFULLY.

EFFECTIVE XXX, 201X

Your health information is personal and private, and we must protect it. This notice tells you how the law requires or permits us to use and disclose your health information, referred to as "Protected Health Information" or "PHI". It also describes your rights and certain obligations we have regarding the use and disclosure of PHI.

Your PHI is information about you, including demographic information that can reasonably identify you, concerning your past, present, or future, physical or mental health condition. The information may be about payment of your health care as well. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires us to keep your PHI private.

All San Bernardino County Department XXX staff, volunteers, interns, contractors, and others, who have access to health information will follow this notice. However, we may change this notice when the law or our practices change. We reserve the right to make the revised or changed notice effective for PHI we already have about you, as well as any information we receive in the future. You will not automatically receive a new notice. If you would like to receive a copy of any new notice, you can access our web site at **www.sbcounty.gov/XXX** or you can request a copy from any XXX staff person.

OUR USES AND DISCLOSURES

How do we typically use or share your health information?

For Treatment: We can use and disclose your PHI to provide you with medical treatment and related services. XXX can share your PHI with doctors, health care personnel, and other staff, who are involved in your care. We can also share your PHI with individuals or entities for your future care for other treatment reasons. We can also use or share your PHI in response to an emergency. For example, a doctor treating you for an injury asks another doctor about your overall health condition.

For Payment: We can use and disclose your PHI to bill and receive payment for the treatment and services you receive. For billing and payment purposes, we can disclose your PHI to your payment source, including insurance or managed care company, Medicare, Medicaid/Medi-Cal, or another third-party payer. For example, we can give your health plan information about the treatment you received so your health plan will pay us or refund us for the treatment. Or, we can contact your health plan to confirm your coverage or to ask for prior authorization for a proposed treatment.

For Health Care Operations: We can use and disclose your information to run our organization and contact you when necessary. This includes quality assurance and improvement actions, reviewing the competence and qualifications of health care professionals, medical review, legal services, audit roles, and general administrative purposes. For example, we can use your PHI to evaluate our services and our staff's performance in caring for you.

There may be some services provided by our business associates, such as a billing service, record storage company, or legal or accounting consultants. We can share your PHI with our business associates so they can perform the job we have asked them to do. We enter into a written contract with our business associates that mandates them to safeguard your information.

For more information see:
www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html

The following describe different ways that we can use or disclose your PHI without obtaining an authorization:

Help with public health and safety issues	• We can share your PHI for certain situations such as: ○ Preventing disease. ○ Helping with product recalls. ○ Reporting adverse reactions to medications. ○ Preventing or reducing a serious threat to anyone's health or safety.
Do research	• We can use or share your PHI for health research.
Comply with the law	We can share your PHI: • As required by federal, state, or local law. • In response to a subpoena, or a court or administrative order. • For workers' compensation claims. • With health oversight agencies for activities authorized by law. • For special government functions such as military, national security, and presidential protective services. • When required to do so by law enforcement officials ○ To identify or locate a suspect, fugitive, material witness, or missing person. ○ About the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement. ○ About a death we believe may be the result of criminal conduct. ○ In emergencies, to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed a crime.
Respond to organ and tissue donation requests and work with a medical examiner or funeral director	• We can share PHI with organ procurement organizations. • We can share PHI with a coroner, medical examiner, or funeral director when an individual dies.

Conduct outreach, enrollment, care coordination, and case management	• We can share your PHI with other government benefits programs like Covered California for reasons such as outreach, enrollment, care coordination, and case management.
Appointment Reminders	• We can use and disclose your PHI to contact you as a reminder that you have an appointment for treatment or care.
Inform individuals involved in your care or payment of your care	• We can share your PHI with a family member, a relative, a friend, or person you identify involved in your medical care or payment provided that you agree to this, or we give you an opportunity to object and you do not do so. If you are unable to agree or object, we may decide that it is in your best interest based on our professional judgment to share your information, such as if you are incapacitated or we need to disclose your PHI in an emergency.
Prevent or report abuse and neglect	• We can share your PHI with a multidisciplinary personnel team relevant to the prevention, identification, management or treatment of an abused child and the child's parents, or elder abuse and neglect.

Additional privacy protections may apply if we are using or sharing sensitive health information, such as HIV-related information, mental health information, psychotherapy notes, and genetic information. For example, under California law, we cannot disclose HIV test results without a written authorization, except in limited circumstances. Your information will be protected according to the highest level of protection required.

**if applicable* We do not create or manage a hospital directory.

YOUR RIGHTS

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get a copy of your health and claims records	• You can ask to see or get a copy of your medical record and other health information we have about you. Ask us how to do this. • We will provide a copy or a summary of your health and claims records, usually within 30 days of your request. We may charge a reasonable, cost-based fee.
Ask us to correct health and claims records	• You can ask us in writing to correct your health and claims records if you think they are incorrect or incomplete. • We can deny your request, but we will tell you why in writing within 60 days.
Request confidential communications	• You can ask us in writing to contact you in a specific way (for example, home or office phone) or to send mail to a different address. • We will consider all reasonable requests and will not ask you the reason for your request.
Ask us to limit what we use or share	• You can ask us in writing not to use or share certain health information for treatment, payment, or our operations. • We are not required to agree; however, if we do agree, we will comply with your request unless your PHI is needed to provide emergency treatment. • If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or operations with your health insurer. We will say “yes” unless a law requires us to share that information.
Get a list of those with whom we have shared information	• You can ask us in writing for a list of disclosures we have made regarding your PHI (accounting of disclosures) up to six years prior to the date of your request. • We will include all the disclosures except for those about treatment, payment, and health care operations, or as required by law. We will provide one accounting per year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

Get a copy of this privacy notice	• You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.
Choose someone to act for you	• If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information. • We will make sure the person has this authority and can act for you before we take any action.
Get a copy of completed test results directly from a laboratory	• You or your authorized personal representative can receive laboratory test results from your health care provider or you can request your completed test report directly from the laboratory that performed the test. • In most cases, laboratories must provide test results within 30 days. • Ask your provider about how to obtain your laboratory results directly.

YOUR CHOICES

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:	• Share information with your family, close friends, or others involved in payment for your care • Share information in a disaster relief situation *If you are not able to tell us your preference, for example if you are unconscious, we can go ahead and share your information if we believe it is in your best interest. We can also share your information when needed to lessen a serious and imminent threat to health or safety.* *Other uses and disclosures of your PHI, not covered by this Notice or the laws that apply to us, will be made only with your written authorization. Please note, you may withdraw authorization for us to use or disclose to others at any time.*

In the case of fundraising:	• We can contact you for fundraising efforts, but you can tell us not to contact you again.

OUR RESPONSIBILITIES

- We are required by law to maintain the privacy and security of your PHI.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We will not use or share your information, other than as described here, unless you tell us we can in writing. If you change your mind at any time, let us know in writing.
- We will never market or sell your information.

For more information visit:
www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html

QUESTIONS OR COMPLAINTS

If you have questions regarding this notice or believe your (or someone else's) rights have been violated, you can contact us or the federal government. We will not retaliate against you for filing a complaint nor will your right to further treatment or future treatment be affected.

For questions regarding this notice or to file a complaint with the San Bernardino County Department of XXX, contact:	San Bernardino County Department of XXX NAME ADDRESS Phone (XXX) XXX-XXXX Email XXX@sbcounty.gov
To file a complaint with the County of San Bernardino, contact:	San Bernardino County HIPAA Complaints 157 West Fifth Street, First Floor San Bernardino, CA 92415 Phone (909) 387-4500 Email HIPAAComplaints@cao.sbcounty.gov
To file a complaint with the Federal Government, contact:	Region IX Office for Civil Rights, Department of Health and Human Services 90 7th Street, Suite 4-100 San Francisco, CA 94103 Phone (800) 368-1019 FAX (415) 437-8329 TDD (800) 537-7697 www.hhs.gov/ocr/privacy/hipaa/complaints/

NOTICE OF PRIVACY PRACTICES: ACKNOWLEDGMENT OF RECEIPT

ACKNOWLEDGMENT OF RECEIPT

By signing this form, you acknowledge receipt of the "Notice of Privacy Practices" of the Department of XXXXXX. Our "Notice of Privacy Practices" tells you how we may use and disclose your protected health information. We encourage you to read it in full.

We may change our "Notice of Privacy Practices." If we change our notice, you may obtain a copy of the revised notice by: accessing our website at XXXXXX or contacting XXXXXXXXX.

If you have any questions about our "Notice of Privacy Practices," please contact: XXXXXXXX

I acknowledge receipt of the "Notice of Privacy Practices" of XXXX

Date:_____

Time:_____AM / PM

Signature: _____

(patient/legal representative)

If signed by someone other than patient, indicate relationship: _____

Print name: _____

(legal representative)

INABILITY TO OBTAIN ACKNOWLEDGMENT

Complete only if no signature is obtained. If it is not possible to obtain the individual's Acknowledgment, describe the good faith efforts made to obtain the individual's Acknowledgment, and the reasons why the Acknowledgment was not obtained.

Patient Name: _____

Reasons why the acknowledgment was not obtained:

- ☐ Patient refused to sign this Acknowledgment even though the patient was asked to do so and the patient was given the Notice of Privacy Practices.
- ☐ Other: _____

Date: _____

Time: _____ AM / PM

Signature: _____

(provider representative)

Print name: _____

(provider representative)