

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration and Governance	Reviewed Date(s):	

Printed copies are for reference only. Please refer to the electronic copy of this document for the latest version.

**Notice:** Under the federal Health Insurance Portability and Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's confidential health information "give way" to those California state law provisions, and other federal provisions, that are more stringent than HIPAA.

**ODCHC staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact your immediate supervisor or the Compliance Officer.**

#### **PURPOSE:**

To address the applicability and responsibilities of business associates, including Omnibus Rule updates. Under the Omnibus Rule of 2013, Business Associates are directly subject to the HIPAA penalties for non-compliance. It also clarifies that Business Associates must comply with the Security Rule and sections of the Privacy Rule. Business Associates must ensure their subcontractors also comply with the HIPAA requirements

#### **DEFINITIONS:**

See HIPAA Compliance Overview policy for all definitions.

#### **POLICY:**

##### General:

- A Business Associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A Business Associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.
- The following organizations are included in the definition of Business Associate:  
A Health Information Organization, E-prescribing gateway, or other person or organization that provides data transmission services with respect to protected health information to ODCHC and that requires routing access to such protected health information.
- A covered entity may be a Business Associate of another covered entity.
- ODCHC may disclose an individual's protected health information to a Business Associate and may allow a Business Associate to create or receive an individual's protected health information to the Business Associate only if:
  - A written contract or agreement is signed by both parties
  - ODCHC has satisfactory assurances that the Business Associate will create, receive, maintain, or transmit electronic protected health information in accordance with 45 CFR 164.

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration and Governance	Reviewed Date(s):	

Printed copies are for reference only. Please refer to the electronic copy of this document for the latest version.

Contract requirements applicable to Business Associates:

- The contract must establish the permitted and required uses and disclosures of protected health information by the Business Associate.
- Not allow the use or further disclosure of protected health information other than as permitted or required by the contract.
- Require the appropriate safeguards to prevent use or disclosure of the protected health information.
- Report to ODCHC any use or disclosure not allowed by the contract of which the Business Associate becomes aware, as required by state and federal regulations including breaches of unsecured protected health information, and any security incident of which it becomes aware.
- Ensure that any agents or subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions and requirements that apply to the Business Associate under the contract, by entering into a contract or other arrangement with the Business Associate.
- Make protected health information in a designated record set available to the individual in accordance with ODCHC policy.
- Make protected health information in a designated record set available for amendment or incorporate any amendments in accordance with ODCHC policy.
- Maintain and make available the information required to provide an accounting of disclosures in accordance with ODCHC policy.
- The Business Associate must make its internal practices, books, and records relating to the use and disclosure of protected health information available to ODCHC and to the DHHS office for the purpose of determining ODCHC compliance with the federal requirements.
- At the termination of the contract, if reasonably feasible, the Business Associate shall recover any protected health information relating to the contract in the possession of its subcontractors, agents, or representatives. The Business Associate shall return or destroy all such ODCHC protected health information relating to the contract and retain no copies.
- Authorize termination of the contract if ODCHC determines that the Business Associate has violated a material term of the contract.

Business Associate Non-Compliance:

If ODCHC knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associates obligation under the contract, ODCHC must take reasonable steps to cure the breach or end the violation, including working with and providing consultation to the Business Associate.

If such steps are unsuccessful, ODCHC must:

- Terminate the contract or agreement; or
- If the termination is not feasible, report the problem to DHHS, Office of Civil Rights.

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration and Governance	Reviewed Date(s):	

Printed copies are for reference only. Please refer to the electronic copy of this document for the latest version.

**REFERENCES:**

*California Hospital Association, California Health Information Privacy Manual, 2017*

*HIPAA rules and regulations, 45 CFR 164*

*County of Sacramento, HIPAA Privacy Rules Policies and Procedures, September 23, 2013*

**ASSOCIATED DOCUMENTS:**

*ODCHC Business Associate Agreement*

*AG\_HIPAA Compliance Overview*

*AG\_De-Identification of PHI and Use of Limited Data Sets*

*AG\_Administrative, Technical, and Physical Safeguards*

*AG\_Use and Disclosure of Protected Health Information*

**KEYWORD TAGS:**

*Business, associate, BAA*