

**DEPARTMENT OF ADMINISTRATIVE SERVICES
DIVISION 55
STATE PURCHASING**

125-055-0100

Purpose – HIPAA Privacy Rule Implementation

The purpose of these rules is to set forth the contract requirements to comply with the Business Associate provisions of The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d –1320d-8, Public Law 104-191, sec. 262 and sec. 264 and the implementing Privacy Rule at 45 CFR part 160 and 164, subparts A and E. The Privacy Rule requires a Covered Entity to obtain certain written assurances from a Business Associate before the Business Associate may disclose, use, or create Protected Health Information. This Rule contains the written assurances that an Agency must include in its Contract with a Business Associate. Before applying this Rule, Agencies must determine if a Business Associate relationship exists between the Contractor and the Agency as defined in HIPAA and the Privacy Rule. The requirements contained in this Rule apply both to Contracts for trade services, as defined in OAR 125-030-0000(57), and to Contracts for personal services, as defined in OAR 125-020-0130.

Stat. Auth.: ORS 184.305, ORS 184.340 and ORS 279.712

Stats. Implemented: ORS 279.712 and The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d –1320d-8, Public Law 104-191, sec. 262 and sec. 264.

125-055-0105

Definitions

For purposes of rules 125-055-0100 through 125-055-0130 the following terms shall have the meanings set forth below. Capitalized terms not defined herein shall have the same meaning as those terms in the Privacy Rule.

(1) “Agency” means any state officer, board, commission, department, institution, branch or agency of the state government that is a Covered Entity under the Privacy Rule and whose costs are paid wholly or in part from funds held in the State Treasury, except the Legislative Assembly, the courts and their officers and committees, and except the Secretary of State and the State Treasurer in the performance of the duties of their constitutional offices.

(2) “Business Associate” means a person or entity who performs or assists a Covered Entity in performing the specific services listed in the HIPAA Privacy Rule, 45 CFR 160.103, where the provision of services involves the use, disclosure, or creation of Protected Health Information by the Contractor. The workforce, as defined in 45 CFR 160.103, of the Covered Entity is not considered to be a Business Associate nor do their activities create a Business Associate relationship with their employer.

(3) “Contract” means the written agreement between an Agency and a Business Associate setting forth the rights and obligations of the parties.

(4) “Covered Entity” means a health plan, a clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction.

(5) “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d – 1320d-8, Public Law 104-191, sec. 262 and sec. 264.

(6) “Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and 164, subparts A and E (2002).

(7) “Rule” means this Oregon Administrative rule 125-055-0100 through 1225-055-0130.

Stat. Auth.: ORS 184.305, ORS 184.340 and ORS 279.712

Stats. Implemented: ORS 279.712 and The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d –1320d-8, Public Law 104-191, sec. 262 and sec. 264.

125-055-0110

References to Privacy Rule

For purposes of this Rule, references to the Privacy Rule mean the final rule published on December 28, 2000 in 65 Fed. Reg. 82,462-82,829, as amended on May 31, 2002 in 67 Fed. Reg. 38,009-38,020 (Part 160) and as amended on August 14, 2002 in 67 Fed. Reg. 53,182-53,273 (Part 160 and 164).

Stat. Auth.: ORS 184.305, ORS 184.340 and ORS 279.712

Stats. Implemented: ORS 279.712 and The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d –1320d-8, Public Law 104-191, sec. 262 and sec. 264.

125-055-0115

Business Associate Contract Provisions

A Contract that is subject to the Business Associate requirements of the Privacy Rule shall contain the following provisions, effective April 14, 2003:

(1) Obligations and Activities of Business Associate: Business Associate agrees to:

(a) Not use or disclose Protected Health Information other than as permitted or required by this Rule and the Contract, or as Required By Law.

(b) Use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Rule and the Contract.

(c) Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Rule and the Contract.

(d) Report to Agency, as promptly as possible, any use or disclosure of the Protected Health Information not provided for by this Rule and the Contract of which it becomes aware.

(e) Ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Agency agrees to the same restrictions and conditions that apply through this Rule and the Contract to Business Associate with respect to such information.

(f) Provide access, at the request of Agency, and in the time and manner designated by Agency, to Protected Health Information in a Designated Record Set, to Agency or, as

directed by Agency, to an Individual in order to meet the requirements under 45 CFR 164.524.

(g) Make any amendment(s) to Protected Health Information in a Designated Record Set that the Agency directs or agrees to pursuant to 45 CFR 164.526 at the request of Agency or an Individual, and in the time and manner designated by Agency.

(h) Make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Agency available to Agency and to the Secretary, in a time and manner designated by Agency or the Secretary, for purposes of the Secretary determining Agency's compliance with the Privacy Rule.

(i) Document such disclosures of Protected Health Information and information related to such disclosures as would be required for Agency to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(j) Provide to Agency or an Individual, in a time and manner to be designated by Agency, information collected in accordance with subparagraph (i) of this section 1, to permit Agency to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(2) Permitted Uses and Disclosures by Business Associate

(a) General Use and Disclosure Provision. Except as otherwise limited in this Rule, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Agency as specified in the Contract and this Rule, provided that such use or disclosure would not violate the Privacy Rule if done by Agency or the minimum necessary policies and procedures of the Agency.

(b) Specific Use and Disclosure Provision.

(A) Except as otherwise limited in this Rule, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(B) Except as otherwise limited in this Rule, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(C) Business Associate may use Protected Health Information to report violations of law to appropriate federal and state authorities, consistent with 45 CFR 164.502(j)(1).

(D) Business Associate may not aggregate or compile Agency's Protected Health Information with the Protected Health Information of other Covered Entities unless the Contract permits Business Associate to perform Data Aggregation services. If the Contract permits Business Associate to provide Data Aggregation services, Business Associate may use Protected Health Information to provide Data Aggregation services requested by Agency as permitted by 45 CFR 164.504(e)(2)(i)(B) and subject to any limitations contained in this Rule. If Data Aggregation services are requested by

Agency, Business Associate is authorized to aggregate Agency's Protected Health Information with Protected Health Information of other Covered Entities that the Business Associate has in its possession through its capacity as a business associate to such other Covered Entities provided that the purpose of such aggregation is to provide Agency with data analysis relating to the Health Care Operations of Agency. Under no circumstances may Business Associate disclose Protected Health Information of Agency to another Covered Entity absent the express authorization of Agency.

(3) Obligations of Agency

(a) Agency shall notify Business Associate of any limitation(s) in its notice of privacy practices of Agency in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information. Agency may satisfy this obligation by providing Business Associate with Agency's most current Notice of Privacy Practices.

(b) Agency shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c) Agency shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Agency has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

(4) Permissible Requests by Agency

Agency shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Agency, except as permitted by section 2(b) above.

(5) Termination of Contract

(a) Termination for Cause. Upon Agency's knowledge of a material breach by Business Associate of the requirements of this Rule, Agency shall either:

(A) Notify Business Associate of the breach and specify a reasonable opportunity in the notice for Business Associate to cure the breach or end the violation, and terminate the Contract if Business Associate does not cure the breach of the requirements of this Rule or end the violation within the time specified by Agency;

(B) Immediately terminate the Contract if Business Associate has breached a material term of this Rule and cure is not possible in Agency's reasonable judgment; or

(C) If neither termination nor cure is feasible, Agency shall report the violation to the Secretary.

(D) The rights and remedies provided herein are in addition to the rights and remedies provided in the Contract.

(b) Effect of Termination.

(A) Except as provided in paragraph (B) of this subsection (b), upon termination of the Contract, for any reason, Business Associate shall return or destroy all Protected Health Information received from Agency, or created or received by Business Associate on behalf of Agency. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(B) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Agency notification of the conditions that make return or destruction infeasible. Upon Agency's written acknowledgement that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Rule to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Stat. Auth.: ORS 184.305, ORS 184.340 & ORS 279.712

Stats. Implemented: ORS 279.712 & The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d–1320d-8, Public Law 104-191, sec. 262 and sec. 264.

125-055-0120

Order of Precedence

In the event of a conflict between this Rule and the provisions of the Contract, this Rule shall control. In the event of a conflict between this Rule and the Privacy Rule or the provisions of the Contract and the Privacy Rule, the Privacy Rule shall control. The requirements set forth in this Rule are in addition to any other provisions of law applicable to the Contract. Provided, however, this Rule shall not supercede any other federal or state law or regulation governing the legal relationship of the parties, or the confidentiality of records or information, except to the extent that HIPAA preempts those laws or regulations. Any ambiguity in the Contract shall be resolved to permit Agency and Business Associate to comply with the Privacy Rule.

Stat. Auth.: ORS 184.305, ORS 184.340 & ORS 279.712

Stats. Implemented: ORS 279.712 & The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d–1320d-8, Public Law 104-191, sec. 262 and sec. 264.

125-055-0125

Methods of Compliance

In addition to incorporating the Business Associate requirements contained in this Rule in its Contracts with Business Associates, Agency may comply with this Rule in either of the following ways:

(1) Memorandum of Understanding

If Agency's Business Associate is also a government entity, the parties may comply with the requirements of this Rule by entering into a memorandum of understanding that accomplishes the objectives of this Rule and meets the Business Associate requirements of the Privacy Rule.

(2) Amendment

Agency may comply with the requirements of this Rule by executing an amendment or rider that amends Agency's Contract with its Business Associate and that contains the contract provisions required by this Rule.

Stat. Auth.: ORS 184.305, ORS 184.340 and ORS 279.712

Stats. Implemented: ORS 279.712 and The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d–1320d-8, Public Law 104-191, sec. 262 and sec. 264.

125-055-0130

Standards in Individual Contracts

- (1) Agency and Business Associate may enter into a Contract that contains more stringent standards than those set forth in this Rule as long as such standards do not violate the requirements of the Privacy Rule.
- (2) State agencies subject to ORS 279.712 shall use the form Contract provided by the State Procurement Office of the Procurement, Fleet, and Surplus Services Division of the Department of Administrative Services (Division). A state agency may request the Division to approve a revised form Contract for repeated use for a specific class or classes of transactions.

Stat. Auth.: ORS 184.305, ORS 184.340 and ORS 279.712

Stats. Implemented: ORS 279.712 and The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d–1320d-8, Public Law 104-191, sec. 262 and sec. 264.