**DEPARTMENT OF ADMINISTRATIVE SERVICES**

**DIVISION 55**

**STATE PURCHASING**

**125-055-0100**

**Purpose — HIPAA Privacy and Security Rule Implementation; HITECH Act Implementation.**

(1) The purpose of these rules is to set forth the requirements that a contractor who is a Business Associate of an Agency must abide by in order to comply with the Business Associate provisions of HIPAA and the implementing Privacy Rule and Security Rule and of the HITECH Act. The Privacy Rule and Security Rule, as amended by the HITECH Act, require an Agency, to obtain certain written assurances from a Business Associate, that the Business Associate will comply with the Business Associate requirements set forth in 45 CFR 164.502(e) and 164.504(e). The Privacy Rule requires that a Covered Entity obtain certain written assurances before the Business Associate may create, receive, maintain or transmit Protected Health Information. The requirements contained in this Rule apply both to Contracts for trade services and personal services, as defined in OAR 125-246-0110.

(2) This Rule will be interpreted as broadly as necessary to implement and comply with HIPAA, the Privacy Rule and the Security Rule, and the HITECH Act. Any ambiguity in this Rule shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the Privacy Rule and the Security Rule, and the HITECH Act.

Stat. Auth.: ORS 184.305, 184.340 & 279A.140
Stats. Implemented: ORS 279A.140 & The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d -1320d-8, PL 104-191, sec. 262 & sec. 264
Hist.: DAS 9-2002(Temp), f. & cert. ef. 12-31-02 thru 6-28-03; DAS 3-2003, f. & cert. ef. 6-27-03; DAS 5-2005(Temp), f. & cert. ef. 4-20-05 thru 10-17-05; DAS 12-2005, f. 10-21-05, cert. ef. 10-22-05; DAS 2-2010(Temp), f. & cert. ef. 7-26-10 thru 1-17-11; DAS 4-2010, f. & cert. ef. 11-15-10; DAS 4-2013, f. 12-17-13, cert. ef. 1-1-14

**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 and the Security Rule and the HITECH Act, including, but not limited to, 42 USC Section 17938 and 45 CFR Section 160.103.

(1) "Agency" means an agency of the State of Oregon subject to the procurement authority of DAS pursuant to ORS 279A.140 and that is:

(a) A Covered Entity; or

(b) A Business Associate of an Agency that is a Covered entity.

(2) "Business Associate" has the meaning given that term in 45 CFR 160.103.

(3) "Contract" means the written agreement between an Agency and a Contractor setting forth the rights and obligations of the parties.

(4) "Covered Entity" has the meaning given that term in 45 CFR 160.103.

(5) “Electronic Media” means:

(a) Electronic storage media; and

(b) Transmission media used to exchange information already in electronic storage media.

(6) “Electronic Protected Health Information” has the meaning given that term in 45 CFR 160.103.

(7) "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.

(8) “HITECH Act” means the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, Title XIII of division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (“ARRA”), Public Law 111-5, including any implementing regulations.

(9) “Health Care Provider” means the persons or entities that furnish, bill for or are paid for Health Care in the normal course of business, as more fully defined in ORS 192.519.

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

(11) “Protected Health Information” has the meaning given that term in 45 CFR 160.103.

(12) “Required by Law” has the meaning given that term in 45 CFR section 164.103.

(13) "Rule" means this Oregon Administrative rule 125-055-0100 through 125-055-0130.

(14) “Secretary” means the Secretary of Health and Human Services (HHS) or any other officer or employee of HHS to whom the authority involved has been delegated.

(15) “Security Rule” means the security standards for Electronic Protected Health Information found at 45 CFR Parts 160, 162, and 164.

Stat. Auth.: ORS 184.305, 184.340 & 279A.140
Stats. Implemented: ORS 192.519; ORS 279A.140 & The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d -1320d-8, PL 104-191, sec. 262 & sec. 264
Hist.: DAS 9-2002(Temp), f. & cert. ef. 12-31-02 thru 6-28-03; DAS 3-2003, f. & cert. ef. 6-27-03; DAS 5-2005(Temp), f. & cert. ef. 4-20-05 thru 10-17-05; DAS 12-2005, f. 10-21-05, cert. ef. 10-22-05; DAS 2-2010(Temp), f. & cert. ef. 7-26-10 thru 1-17-11; DAS 4-2010, f. & cert. ef. 11-15-10; DAS 4-2013, f. 12-17-13, cert. ef. 1-1-14

**125-055-0115**

**Business Associate Contract Provisions**

(1) A Contractor that is a Business Associate of an Agency must:

(a) Not use or disclose Protected Health Information or Electronic 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 and Electronic 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 or Electronic 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 or Electronic 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 or Electronic Protected Health Information created, received, maintained or transmitted by it 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 or Electronic 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 or Electronic 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 relating to the use and disclosure of Protected Health Information and Electronic Protected Health Information created, received, maintained or transmitted 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 or Security Rule.

(i) Document disclosures of Protected Health Information and Electronic 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 and Electronic 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 subsection (i) of this section to permit Agency to respond to a request by an Individual for an accounting of disclosures of Protected Health Information and Electronic Protected Health Information in accordance with 45 CFR 164.528.

(2) A Contractor that is a Business Associate of an Agency may, except as otherwise limited or prohibited by this Rule:

(a) Use or disclose Protected Health Information and Electronic 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, Security Rule, the HITECH Act, or other applicable federal or state laws or regulations if done by Agency or the minimum necessary policies and procedures of the Agency. All other uses of Protected Health Information and Electronic Protected Health Information are prohibited.

(b) Use Protected Health Information and Electronic Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(c) Disclose Protected Health Information and Electronic Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law.

(d) Disclose Protected Health Information and Electronic Protected Health Information to a subcontractor if the Business Associate enters into a business associate agreement with that subcontractor that complies with this Rule.

(e) Use Protected Health Information and Electronic Protected Health Information to report violations of law to appropriate federal and state authorities, consistent with 45 CFR 164.502(j)(1).

(3) A Contractor that is a Business Associate of an Agency may not aggregate or compile Agency's Protected Health Information or Electronic Protected Health Information with the Protected Health Information or Electronic 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 Heath 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.

(4) Obligations of Agency:

(a) An Agency that has entered into a Contract with a Business Associate shall notify Business Associate of any:

(A) 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 and Electronic Protected Health Information. Agency may satisfy this obligation by providing Business Associate with Agency's most current Notice of Privacy Practices.

(B) Changes in, or revocation of, permission by Individual to use or disclose Protected Health Information or Electronic Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information and Electronic Protected Health Information.

(C) Restriction to the use or disclosure of Protected Health Information or Electronic 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 or Electronic Protected Health Information.

(b) Agency shall not request Business Associate to use or disclose Protected Health Information or Electronic Protected Health Information in any manner that would not be permissible under the Privacy Rule or Security Rule if done by Agency, except as permitted by section (1)(b)(B) above.

(5) Security Requirements. A Business Associate of an Agency is subject to the Security Rule’s Business Associate requirements for Electronic Protected Health Information and must comply with both the Privacy Rule and the Security Rule requirements applicable to a Business Associate. In addition to the Privacy Rule requirements set forth in this Rule, the Contractor must:

(a) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the Agency, and develop and enforce related policies, procedure, and documentation standards (including designation of a security official).

(b) Ensure that any agent, including a subcontractor, to whom it provides Electronic Protected Health Information agrees to implement reasonable and appropriate safeguards to protect it by entering into a business associate agreement; and

(6) Breach.

(a) In the event of Discovery of a Breach of Unsecured Protected Health Information a Business Associate of an Agency must:

(A) Notify the Agency of such Breach. The notification of a Breach to the Agency must be made as soon as possible and Business Associate shall confer with the Agency as soon as practicable thereafter, but in no event, shall notification to the Agency be later than 30 calendar days after the Discovery of a Breach. Notification shall include identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired or disclosed during such Breach and any other information as may be reasonably required by the Agency necessary for the Agency to meet its notification obligations;

(B) Confer with the Agency as to the preparation and issuance of an appropriate notice to each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired or disclosed as a result of such Breach;

(C) Where the Breach involves more than 500 individuals, confer with the Agency as to the preparation and issuance of an appropriate notice to prominent media outlets within the State or as appropriate, local jurisdictions; and,

(D) Confer with the Agency as to the preparation and issuance of an appropriate notice to the Secretary of Unsecured Protected Health Information that has been acquired or disclosed in a Breach. If the Breach was with respect to 500 or more individuals, such notice to the Secretary must be provided immediately. If the Breach was with respect to less than 500 individuals, a log may be maintained of any such Breach and the log must be provided to the Secretary annually documenting such Breaches occurring during the year involved.

(b) Except as set forth in (c) below, notifications required by this section must be made without unreasonable delay and in no case later than 60 calendar days after the Discovery of a Breach. Any notice must be provided in the manner and content required by the HITECH Act, sections 13402(e) and (f), and 45 CFR 164.404–164.410.

(c) Any notification required by this section may be delayed by a law enforcement official in accordance with the HITECH Act, section 13402(g).

(d) For purposes of this section, the terms “Breach” and “Unsecured Protected Health Information” have the meaning set forth in 45 CFR 164.402. A Breach will be considered as “Discovered” in accordance with the HITECH Act, section13402(c), 45 CFR 164.404(a)(2), and 45 CFR 164.410(a)(2).

(7) Violations of this Rule.

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

(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.

(b) The rights and remedies provided in this Rule are in addition to the rights and remedies provided in the Contract.

(c) Effect of Termination.

(A) Except as provided in subsection (c)(B) below upon termination of the Contract, for any reason, Business Associate shall, at Agency’s option, return or destroy all Protected Health Information and Electronic 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 and Electronic 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 and Electronic Protected Health Information.

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

Stat. Auth.: ORS 184.305, 184.340 & 279A.140
Stats. Implemented: ORS 279A.140 & The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d -1320d-8, PL 104-191, sec. 262 & sec. 264
Hist.: DAS 9-2002(Temp), f. & cert. ef. 12-31-02 thru 6-28-03; DAS 3-2003, f. & cert. ef. 6-27-03; DAS 5-2005(Temp), f. & cert. ef. 4-20-05 thru 10-17-05; DAS 12-2005, f. 10-21-05, cert. ef. 10-22-05; DAS 2-2010(Temp), f. & cert. ef. 7-26-10 thru 1-17-11; DAS 4-2010, f. & cert. ef. 11-15-10; DAS 4-2013, f. 12-17-13, cert. ef. 1-1-14

**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 Security Rule or the HITECH Act, or the provisions of the Contract and the Privacy Rule or the Security Rule or the HITECH Act, the Privacy Rule and the Security Rule and the HITECH Act 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 and the HITECH Act preempt those laws or regulations. Any ambiguity in the Contract shall be resolved to permit Agency and Business Associate to implement and comply with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule.

Stat. Auth.: ORS 184.305, 184.340 & 279A.140
Stats. Implemented: ORS 279A.140 & The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d -1320d-8, PL 104-191, sec. 262 & sec. 264
Hist.: DAS 9-2002(Temp), f. & cert. ef. 12-31-02 thru 6-28-03; DAS 3-2003, f. & cert. ef. 6-27-03; DAS 5-2005(Temp), f. & cert. ef. 4-20-05 thru 10-17-05; DAS 12-2005, f. 10-21-05, cert. ef. 10-22-05; DAS 2-2010(Temp), f. & cert. ef. 7-26-10 thru 1-17-11; DAS 4-2010, f. & cert. ef. 11-15-10; DAS 4-2013, f. 12-17-13, cert. ef. 1-1-14

**125-055-0125**

**Methods of Compliance**

In addition to referencing compliance with this Rule in a Contract with a Business Associate, Agency may comply with this Rule in any of the following ways:

(1) Memorandum of Understanding. If a Business Associate is 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 and the Security Rule.

(2) Amendment. Agency may comply with the requirements of this Rule by executing an amendment or rider that amends Agency's Contract and that contains the contract provisions required by this Rule.

(3) Required by Law. If a Business Associate is Required by Law to perform a function or activity on behalf of an Agency or to provide a service described in the definition of Business Associate to an Agency, such Agency may disclose Protected Health Information to the Business Associate to the extent necessary to comply with the legal mandate without meeting the requirements of this Rule, provided that the Agency attempts in good faith to obtain satisfactory assurances required by OAR 125-055-0115, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

Stat. Auth.: ORS 184.305, 184.340 & 279A.140
Stats. Implemented: ORS 279A.140 & The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d -1320d-8, PL 104-191, sec. 262 & sec. 264
Hist.: DAS 9-2002(Temp), f. & cert. ef. 12-31-02 thru 6-28-03; DAS 3-2003, f. & cert. ef. 6-27-03; DAS 5-2005(Temp), f. & cert. ef. 4-20-05 thru 10-17-05; DAS 12-2005, f. 10-21-05, cert. ef. 10-22-05; DAS 2-2010(Temp), f. & cert. ef. 7-26-10 thru 1-17-11; DAS 4-2010, f. & cert. ef. 11-15-10; DAS 4-2013, f. 12-17-13, cert. ef. 1-1-14

**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 or the Security Rule or the HITECH Act.

(2) Agencies shall use one of the forms provided or approved by the Department of Administrative Services when entering into personal services contracts as defined in OAR 125-246-0110. For revised forms up to a cumulative value of $150,000 and before an Agency may use a revised form, it must obtain its Designated Procurement Officer’s approval of any revisions to the form’s terms and conditions. For revised forms exceeding a cumulative value of $150,000 and before an Agency may use a revised form, it must obtain Department of Justice approval of any revisions to the revised form’s terms and conditions.

Stat. Auth.: ORS 184.305, 184.340 & 279A.140
Stats. Implemented: ORS 279A.140 & The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d -1320d-8, PL 104-191, sec. 262 & sec. 264
Hist.: DAS 9-2002(Temp), f. & cert. ef. 12-31-02 thru 6-28-03; DAS 3-2003, f. & cert. ef. 6-27-03; DAS 5-2005(Temp), f. & cert. ef. 4-20-05 thru 10-17-05; DAS 12-2005, f. 10-21-05, cert. ef. 10-22-05; DAS 2-2010(Temp), f. & cert. ef. 7-26-10 thru 1-17-11; DAS 4-2010, f. & cert. ef. 11-15-10; DAS 4-2013, f. 12-17-13, cert. ef. 1-1-14