SUBJECT: BUSINESS ASSOCIATES

GENERAL STANDARD (PRIVACY RULE SECTIONS 164.502(e) and 164.504(e)):

AHS health care providers and health plans are required to have certain contracts or other arrangements in place with their Business Associates, as required by the Privacy Rule.

AHS will utilize a form Business Associate agreement (or a memorandum of understanding, if applicable) that satisfies the requirements of Section 164.504(e) of the Privacy Rule. The Business Associate agreement will impose confidentiality and other obligations on the Business Associates.

PRIVACY RULE:

I. Valid Business Associate Contracts

A. A Business Associate (BA) contract must:

1. Delineate all permitted and required uses and disclosures of PHI by the BA;

2. Prohibit any use or disclosure of PHI by the BA in a manner that would violate the Privacy Rule if done by the CE, except that:

   a. The contract may permit the BA to provide data aggregation services relating to the health care operations of the CE;

   b. The contract may permit the BA to use the information received by the BA in its capacity as a BA to the CE, if necessary, for the proper management and administration of the BA or to carry out the legal responsibilities of the BA; and

   c. The contract may permit the BA to disclose the information received by the BA in its capacity as a BA for the proper management and administration of the BA or to carry out the legal responsibilities of the BA, if: the disclosure is required by law or the BA obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially 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 BA of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Authorize termination of the contract by the CE, if the CE determines that the BA has violated a material term of the contract;

4. Provide that the BA will:

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

   b. Use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by its contract;

   c. Report back to the CE of any use or disclosure of PHI which is <u>not</u> provided for in the contract, of which the BA becomes aware;

   d. Ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the BA on behalf of, the CE agrees to the same restrictions and conditions that apply to the BA with respect to such information;

   e. Make available PHI in accordance with Section 164.524 of the Privacy Rule (See, the General Standard and Guidelines on "Access");

   f. Make available PHI for amendment and incorporate any amendments to PHI in accordance with Section 164.526 of the Privacy Rule (See, the General Standard and Guidelines on "Amendment");

   g. Make available the information required to provide an accounting of disclosures in accordance with Section 164.528 of the Privacy Rule (See, the General Standard and Guidelines on "Accounting");

   h. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the BA on behalf of, the CE available to the Secretary of Health and Human Services for purposes of determining the CE's compliance with the Privacy Rule; and

   i. At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the BA on behalf of, the CE that the BA 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.

II. <u>Arrangements other than Business Associate Contracts</u>

A. If a CE and its BA are both governmental entities:

   1. The CE may comply with the requirement to have a BA contract by entering into a memorandum of understanding with the BA that contains

the terms that accomplish the objectives of the terms required to be in the BA contract.

2. The CE may comply with the requirement to have a BA contract, if other law (including regulations adopted by the CE or its BA) contains requirements applicable to the BA that accomplish the objectives of the terms required to be in the BA contract.

B. If a BA is required by law to perform a function or activity on behalf of a CE or to provide a service described in the definition of "Business Associate" to a CE, such CE may disclose PHI to the BA to the extent necessary to comply with the legal mandate without meeting the requirements to have a BA contract, provided that the CE attempts in good faith to obtain a BA contract or other arrangement, and, if such attempt fails, documents the attempt and the reasons for the failure.

C. The CE may omit from the arrangements set forth in Paragraph A above the termination authorization required in Paragraph I.A.3. above, if such authorization is inconsistent with the statutory obligations of the CE or its BA.

III. Other Business Associate Contract Guidelines

A. No BA contract is necessary:

1. With respect to disclosures by the CE to a health care provider concerning the treatment of the individual; or

2. With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the PHI used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

B. A CE is not in compliance with the Privacy Rule if the CE knew of a pattern of activity or practice of the BA that constituted a material breach or violation of the BA's obligations under the contract or other arrangement, unless the CE took reasonable steps to cure the breach or end the violation, and if such steps were unsuccessful:

1. The CE terminated the contract or arrangement, if feasible; or

2. If termination is not feasible, the CE reported the problem to the Secretary of Health and Human Services.

IV. CE as a BA of Another Covered Entity

If a CE violates its contractual obligations as a BA of another covered entity, then the CE will be deemed to have violated the Privacy Rule.

V. CE with Multiple Covered Functions

A. If a CE performs multiple covered functions that would make the CE any combination of a health plan, a covered health care provider, and a health care clearinghouse, then the CE must comply with the Privacy Rule, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

B. If a CE performs multiple covered functions, it may use or disclose the PHI of individuals who receive the CE's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

GUIDELINES:

1. AHS health care providers and health plans have identified potential Business Associates, and have worked to ensure they have appropriate contractual terms in place with each.

2. AHS understands that in some situations, the compliance date for having Business Associate agreements in place was not April 14, 2003. More specifically, Section 164.532(d) and (e) of the Privacy Rule provide a limited extension with respect to Business Associate obligations. Generally, the extension only applies if an underlying agreement (e.g., a services agreement) with a Business Associate was in place as of October 15, 2002, and if that agreement had not been modified or renewed (other than through an "evergreen" or, automatic, renewal) between October 15, 2002 and April 14, 2003. In that event, the compliance date for entering into the Business Associate agreement would be extended until such time as the underlying agreement was renewed or modified, but in no event later than April 14, 2004. AHS is also aware that even when the extension applies, it must still ensure that the Business Associate cooperates with AHS in the context of an HHS enforcement review or investigation, when an individual seeks to exercise rights to access PHI, amend PHI, or obtain an accounting of disclosures of PHI, and when a violation of the Privacy Rule, or of the AHS Standards and Guidelines, occurs (to mitigate the violation).

3. A copy of a form stand-alone Business Associate agreement that is available for use by AHS health care provides and health plans is attached to this Standard and Guidelines. In this context, "stand-alone" means the agreement is not physically incorporated into an underlying services agreement with a Business Associate. The attached form can be modified for use as an exhibit to an underlying services agreement.

4. AHS has provided training to those groups who might be responsible for the development, negotiation, and execution of Business Associate agreements. In particular, AHS has provided training to representatives of each of its Departments, Divisions, and Offices that might have need to enter into a Business Associate agreement, and to the attorneys (e.g., Assistant Attorneys General) who might be called upon to review these agreements. The training has focused on the identification of Business Associates, and

the specific obligations Business Associates are required to accept under the Privacy Rule. AHS has provided such departments with form language to be used to capture Business Associate requirements (see the form agreement attached below).

5. AHS has provided training to the aforementioned groups to ensure that such groups are aware of the steps AHS must take if and when they learn of any breach of the Business Associate terms by a Business Associate. In that regard, all such persons have been trained to promptly notify the Privacy Official of any such breach, and to then work closely with the Privacy Official on the resolution of such breach. The Privacy Official will closely monitor the return or destruction of PHI used, created or obtained by the Business Associate upon termination of a contract.

6. AHS has also provided training to the aforementioned groups to ensure that such groups are aware of the requirements that AHS must accept, if and when AHS is a Business Associate of another covered entity under the Privacy Rule.

7. AHS is aware that in some situations, its health care providers and health plans receive "Business Associate" support from other State of Vermont agencies (or the departments, divisions or offices of such agencies). More specifically, these other state agencies perform or assist in the performance of functions or activities on behalf of AHS, or perform services for AHS, that would make the other agency a HIPAA Privacy Rule Business Associate. For example, the Agency of Administration, through its Department of Buildings and General Services, performs document storage and shredding services for AHS health care providers and health plans, and in performing these roles, is acting as a Business Associate to AHS. For another example, Assistant Attorneys General provide legal services to many of the Departments, Divisions and Offices within AHS and in performing these services, the Assistant Attorneys General are acting as Business Associates to AHS.

8. AHS has identified, and will continue to identify, those situations where it receives "Business Associate" support from other State of Vermont agencies, or the departments, divisions or offices that comprise those agencies. In those situations, AHS will enter into a memorandum of understanding ("MOU") with the other agency, with such MOU containing substantially all of the terms and conditions identified in the attached form stand-alone Business Associate agreement. AHS is aware that Section 164.504(e)(3)(i)(A) of the Privacy Rule permits the use of an MOU (as opposed to a more formal contract) in these circumstances. In addition, and to the greatest extent possible, AHS will enter into a single MOU with the other agency that covers all of the AHS Departments, Divisions, and Offices, so as to preclude the necessity for multiple MOUs addressing the same Business Associate issues.

9. AHS also recognizes that in some situations, a specific health care provider or health plan may receive "Business Associate" support from another Department, Division or Office of AHS. For example, the Disability Determinations Division ("DDD") performs Medicaid eligibility determinations for PATH. In these situations, a Business Associate agreement or MOU will not be necessary, because the Department, Division or Office is a part of the workforce of AHS (e.g., because DDD is an AHS Division). In addition, and as it concerns eligibility determinations, Section 164.502(e)(1)(ii)(C) of the Privacy Rule arguably obviates the need for a Business Associate agreement between one Department, Division or Office of AHS and another (consequently, this is a further

reason why a Business Associate agreement or MOU would not be required between AHS and DDD).

10. The form agreement attached below also includes provisions required by the HIPAA Security Rule (See, Section 14). AHS will endeavor to identify those situations where it has used form Business Associate agreements that did not include these "Security Rule provisions", such that it can amend those agreements prior to the April 21, 2005 Security Rule compliance date.

11. AHS has instructed its workforce members that they should not execute Business Associate agreements provided by third parties without first having those agreements reviewed, and potentially modified, by the Assistant Attorney General or other counsel providing services to the Department, Division, or Office at issue.

12. AHS does have group health plans that are covered by the Privacy Rule. Such plans are addressing their separate compliance obligations under the Privacy Rule.