

Department of Public Health and
Human Services (DPHHS)

Health Insurance Portability
and Accountability Act
("HIPAA") Privacy Policy

Laurie Lamson,
Operations Services Branch Manager

Revised Date:

Legal Citations: Health Insurance Portability and Accountability Act ("HIPAA"), HiTech Act of the American Recovery and Reinvestment Act ("ARRA") of 2009 (Social Security Act Sections 1171-1180, 42 USC 1320d- 1320d (9)), 45 CFR 164.302 et seq.

Policy Title:	Business Associate Agreements		
Policy Number:	015	Version:	2.0 revised
Approved By:			
Original Effective Date	February 27, 2003		
Revised Effective Date:	January 1, 2010		

Purpose:

This policy addresses the agreements necessary to secure Protected Health Information (PHI) that is entrusted to individuals and agencies contracted as business associates of DPHHS.

Policy:

Business associates are by definition a covered entity and must follow HIPAA and American Recovery and Reinvestment Act ("ARRA") guidance. Business associates of DPHHS who require PHI to perform work related to DPHHS's role as a covered entity must have that role detailed in a business associate agreement.

Definition:

Business associate – A person or organization that performs a function on behalf of DPHHS that requires the use or disclosure of PHI and is related to the health care component activities of DPHHS. Such functions may include claims processing, utilization review, quality assurance, billing, benefits management, legal, actuarial, accounting, consulting, data aggregation, management, administration, accreditation, disposal of PHI in paper or electronic formats, or financial services. Business associates do not include members of the DPHHS workforce.

- 1 Business associate agreements must specify the uses and disclosures of PHI that DPHHS requires of the business associate. The agreement will state that the business associate must comply with all applicable HIPAA policies and conduct its business as a covered entity.
- 2 The agreement will assure that the business associate:

- a. Will not use or further disclose the information other than as permitted by the contract or required by law;
 - b. Will use appropriate safeguards to protect PHI;
 - c. Will report any use or disclosure not provided for in the agreement immediately upon discovery of a breach or release of unsecured protected health information; no later than 30 days from the discovery to allow for notification to individuals, the media and the Secretary of Health and Human Services within the 60 day allowed time frame imposed by ARRA by DPHHS or the business associate as dictated in the contract;
 - d. Will ensure that any agents or subcontractors used by the business associate will also apply the appropriate safeguards required by the business associate agreement;
 - e. Will provide a mechanism by which PHI is made available to the client for review, copying, or amendment and will make available the information necessary to account for these disclosures;
 - f. Will make its internal practices and records available to the Secretary of Health and Human Services for purposes of determining compliance with HIPAA and ARRA; and
 - g. At the termination of the contract, if feasible, return or destroy all PHI received from or created for DPHHS.
- 3 If DPHHS becomes aware of any practices of the business associate that constitute a material breach of the agreement, DPHHS must take steps to correct or end the violation. If such steps are unsuccessful, DPHHS must either terminate the contract or, if that is not feasible, report the problem to the Secretary of Health and Human Services.
 - 4 DPHHS is not required, however, to monitor the privacy practices of the business associate and is not liable for privacy breaches of the business associate.
 - 5 PHI disclosed to a business associate for purposes of treatment, payment or healthcare operations may not require an accounting to the client, depending on the nature of the PHI.