HIPAA PRIVACY & SECURITY POLICY

The Health Insurance Portability and Accountability Act of 1996, also known as "**HIPAA**," provides federal regulations for protecting the privacy and security of personal health information. Benefit Administration by Design LLC ("**BABD**"), in its capacity as a third party administrator for employer group health plans, is committed to protecting employees' and their family members' personal health information. BABD will only use and disclose individual personal health information it receives from clients as necessary to perform the duties for which BABD has been engaged by the client. BABD seeks to satisfy or surpass the HIPAA regulatory standards and has adopted written HIPAA privacy and security policies to accomplish this goal. These HIPAA privacy and security procedures are available upon request.

SCOPE OF THE HIPAA PRIVACY AND SECURITY RULES

HIPAA provides federal privacy standards to protect individuals' medical records and other health information ("**PHI**") provided to health plans, doctors, hospitals, other health care providers ("**Covered Entities**") and businesses who provide services to Covered Entities, known as Business Associates, such as BABD as a third party administrator. These rules limit the purposes to which individuals' PHI can be disclosed – in the case of a group health plan such disclosures generally are limited to treatment, payment or health care operations. However, certain disclosures of PHI may be made for public health and safety reasons. HIPAA also requires Covered Entities to protect the security and confidentiality of health information they transmit in electronic form ("**ePHI**"). Most health plans, hospitals, health insurers, pharmacies, doctors and other health care providers are required to comply with HIPAA's requirements. The rules apply equally to private sector and public sector covered entities. For additional information about the HIPAA regulations, see the HHS web site at: www.hhs.gov/ocr/hipaa.

Notice of Privacy Practices: Covered Entities must provide a notice to individuals about how their PHI may be used and their rights under the HIPAA privacy regulation. Group health plans should provide individuals a copy of this notice when individuals enroll in the Plan. Doctors, hospitals and other direct-care providers generally will provide the notice on the individual's first visit. Individuals may also request a copy of the notice.

Individual Protections: To provide individuals more control over how their PHI is used and disclosed, HIPAA provides individuals with the following rights:

- **Access to Medical Records:** Individuals generally can view and obtain copies of their medical records and request corrections if they identify errors or mistakes. Covered Entities, or

Business Associates on their behalf, typically must provide access to these records within 30 days, and may charge individuals for the cost of copying and sending the records.

- **Confidential Communications:** Under the privacy rule, individuals can request that their health plans, medical providers and other covered entities take reasonable steps to ensure that their communications are confidential. For example, an individual could as the plan administrator of his group health plan to call his or her office rather than home, and the plan should comply with that request if it can be reasonably accommodated.
- **Complaints:** Individuals may file a formal complaint regarding a health plan's or other covered entity's privacy practices. Such complaints can be made directly to health plan/covered entity or to the Health and Human Services' Office for Civil Rights which is charged with investigating complaints and enforcing the privacy regulation. Information about filing complaints should be included in each covered entity's notice of privacy practices. Individuals can find out more information about filing a privacy-related complaint by contacting:

Department of Health and Human Services
(866) 627-7748 or //www.hhs.gov/ocr/hipaa

Covered Entities' Responsibilities: The privacy rule requires health plans, pharmacies, doctors and other covered entities to establish policies and procedures to protect the confidentiality of individual's PHI and ePHI. These requirements are flexible and scalable to allow different covered entities to implement them as appropriate for their businesses and practices and will evolve as technologies and operational requirements change. Covered entities generally must take steps to ensure that any business associates who have access to PHI and ePHI agree to the same limitations on the use and disclosure of that information.

- **Written Privacy Procedures:** Covered entities must have written privacy procedures that describe how and when PHI may be used and disclosed. These procedures must identify the employees that have access to PH and ePHI (referred to as "**workforce members**").
- **Employee Training and Privacy Officer:** Covered entities must provide HIPAA training to workforce members and must designate a privacy officer to be responsible for ensuring the procedures are followed. If covered entities learn that a workforce member failed to follow these procedures, they must take appropriate disciplinary action.
- **Implement Security Measures:** Covered entities must implement appropriate security measures to ensure the confidentiality, integrity, and availability of ePH they create, receive, maintain, or transmits. The security rules do not mandate Covered Entities to adopt specific technologies but rather permit Covered Entities to adopt security measures that are appropriate given their size, capabilities, the costs of the specific security measures and the operational impact. The security rule distinguishes between implementation specifications that are required and those that are addressable. In some cases, a Covered Entity may choose not to implement an addressable specification at all if it can demonstrate that both the specification and alternative measures are not reasonable or appropriate. However, those measures adopted must protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI and must protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required.

  The security standards cover three main categories:

(i) ***Administrative safeguards*** that specify the administrative functions that should be implemented to meet the security standards. They include assignment or delegation of security responsibility to an individual and security training requirements for workforce members.

(ii) ***Physical safeguards*** that are the mechanisms required to protect electronic systems, equipment and the data they hold from threats, environmental hazards and unauthorized intrusion. They include restricting access to ePHI, retaining off site computer backups and disaster recovery procedures.

(iii) ***Technical safeguards*** that are the automated processes used to protect data and control access to data. They include using authentication controls to verify that the person signing onto a computer is authorized to access that ePHI, or encrypting and decrypting data as it is being stored and/or transmitted.

BABD WEBSITE

Website Operations

BABD considers information submitted to it through our website to be private and confidential. Only designated employees have access to individual information that is submitted and we make extensive efforts to keep data secure. BABD may contact individuals who make requests through our website site, based on contact information they provide. We do so only when necessary to appropriately complete an individual request.

No Third Party Information Sharing

BABD does not share e-mail addresses or any other information with third parties. We will never share personal data with unrelated outside entities or other businesses.

Visitor Tracking

BABD does not take any steps to obtain personal data about visitors to our website via web tracking. We check the number of visitors to our site and compile statistics about our web traffic but we do not attempt in any way to determine personal data about site visitors unless they choose to submit information to us through the website.

Outside links

As a resource to our clients and visitors, BABD may post articles that may include links to outside websites. BABD cannot assume responsibility for privacy policies of other websites.

Site Sponsorship and Advertising Policy

BABD provides its website as a resource for its clients and is the sole sponsor of the website contents. BABD does not provide third party advertising through its website. Any banners or promotions are for BABD-related events, activities or services.