Health Insurance Portability and Accountability Act (HIPAA)

A. The Privacy Regulation

The HIPAA Privacy Regulations, with a compliance date of April 14, 2003, mandates that all Protected Health Information (PHI) be secured from use for reasons other than Medical Payments, Treatments, or Health Care Operations (PTO). Employee Benefits Division (EBD) is considered a health plan and therefore is subject to the Privacy Regulation and bound to secure and protect all enrollees' health information. Protecting this information includes limiting uses and disclosures in all forms to those individuals not directly involved in services for PTO. For this reason, EBD has chosen to use ARBenefits Call System (a secure messaging system) for questions regarding PHI.

B. The Security Regulation

The HIPAA Security Regulations, with a compliance date of April 14, 2005, mandates that all electronically transferred Protected Health Information (PHI) be secured. For this reason, EBD has chosen to use ARBenefits Task System (an encrypted email system for EBD employees, contract workers, business associates, and carriers for questions regarding PHI and File Transfer Protocol (FTP), a secure website, for the transfer of PHI to and from our health carriers and vendors).

C. How HIPAA Affects EBD

Compliance

EBD is considered a health plan administrator under HIPAA Privacy Regulations and is therefore subject to the privacy and security sections of these regulations.

The Privacy/Security Regulations have specific tasks and accomplishments, which must be in place in order for a Covered Entity to be considered compliant. EBD has complied with these requirements as detailed in the following list:

1. Appointment of a Privacy/Security Officer:
   The Privacy/Security Officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to EBD's policies and procedures covering the privacy and security of and access to patient health information in compliance with federal and state laws.
2. Notice of Privacy Practices (NPP) to all plan participants:
   The NPP is available on the EBD web site and must be provided to all new enrollees in the plan. EBD accomplishes this by distributing the NPP via the Summary Plan Description (SPD) and Guide to Enrollment.
3. Policies regarding disclosures of PHI:
   EBD has policies and procedures in place addressing the use and disclosure of PHI. These policies and procedures are accessible and available upon request to all enrollees, and Insurance Representatives.

4. Training for relevant employees:
   EBD is responsible for providing oversight, training, auditing, investigating and reporting of HIPAA-related policy, procedures, issues and violations for all members, business affiliates and business partners of the State of Arkansas State and Public School Employees Life and Health Insurance plan.

D. Uses and Disclosures of PHI

1. Authorization for uses and disclosures outside of PTO:
   Plan enrollee information can only be used and disclosed by EBD for purposes related to payment of claims, medical treatment, and health care operations. Communication between health carriers, prescription benefits manager, providers, and EBD is allowed for the above stated reasons without the enrollee's consent. Written authorization is required from the enrollee in order for EBD staff to disclose an enrollee's health information with anyone outside PTO. This includes health insurance representatives, payroll personnel, family members, legal counsel, and friends. Authorization forms are available at EBD and are specific to the situation being addressed, applicable to the person listed as authorized to discuss the enrollee's information and valid only until the expiration date on the form.
2. Identification of employees who may receive PHI:
   EBD has identified specific employees within EBD, who are able to use and disclose member's medical information. A listing of these individuals has been provided to each of our carriers and is updated quarterly.
3. Restriction of access to information:
   EBD has restricted access to certain levels of information. Access to information is based on a minimum necessary for job function.
4. Employee Non-compliance:
   EBD has discipline policies and procedures in place for staff that do not follow privacy or security procedures. A suspected breach of confidentiality or possible unlawful disclosure should be reported to the EBD Privacy/Security Officer for investigation within one (1) business day.

E. How HIPAA Affects Insurance Representatives

1. Health Insurance Representatives are required to verify their identity any time that they contact EBD for security purposes. Representatives must answer two (2) out of four (4) questions correctly in order to verify their identity. Questions that must be answered are, Name, Social Security Number, Group ID, and Pin # (or your login ID).
2. Discussion and/or communication of an enrollee's PHI between EBD staff and Health Insurance Representatives will no longer be allowed without a member's specific written authorization allowing the named Health Insurance Representative (HIR) access to the enrollee's PHI.

3. If an Insurance Representative receives authorization to provide an enrollee's health information, the representative becomes responsible to secure and protect that enrollee's health information from all others not involved in the member's health care. You must not discuss a member's Protected Health Information (PHI) with any individual other than the member without a member's specific written authorization.
4. All health information must be separate from all employment documents and must not be accessible to any unauthorized person. Directors, Superintendents, Principals, and other supervisors do not have a right to an employee's heath Information. Should this occur the Insurance Representative might be liable for the violation. You are responsible for securing and protecting any PHI to which you are given access.
5. Business Affiliates will complete all Business Associate Agreements and Confidentiality statements as requested by EBD in timely manner. Any personnel changes must be reported to EBD within five (5) business days.
6. Business Affiliates will be subject to reasonable audit to ensure compliance with HIPAA regulations.
7. Business Affiliates must report any suspected violations or breaches to EBD Security for investigation within one (1) business day.

Note: Please encourage the employees to call the insurance carriers or EBD directly to resolve claim problems. If these attempts are unsuccessful then they may contact the Insurance Representative for assistance. Please remember to obtain signed authorization (and forward a copy to EBD).

F. Penalties for Non-Compliance or Violations

The Privacy and Security Regulations are monitored and enforced by The Federal Department of Health and Human Services (HHS), Office of Civil Rights (OCR). Penalties for non-compliance are as follows:

Civil Money Penalties

- $100 to $50,000 for each violation where the entity did not know (even with reasonable diligence) that they were in violation of the statute, with a $25,000 to $1.5 million cap per year for violating the same requirement,
- $1,000 to $50,000 for each violation where the entity had reasonable cause, but did not show willful neglect in violating the law, with a $100,000 to $1.5 million cap per year for violating the same requirement,
- $10,000 to $50,000 for each violation where the entity showed willful neglect of the law, but corrected the violation within 30 days of discovery, with a $250,000 to $1.5 million cap per year for violating the same requirement,
- $50,000 for each violation where the entity showed willful neglect of the law, but failed to correct the violation within 30 days of discovery, with a $1.5 million cap per year for

violating the same requirement, However, there is no maximum penalty for this circumstance.

Criminal Penalties

- Fine of up $50,000 and up to one (1) year in jail for knowingly disclosing individually identifiable health information
- Fine of up to $100,000 and up to five (5) years for offenses committed under false pretenses
- Fine of up to $250,000 and up to ten (10) years for offenses committed for personal gain or with malicious intent

Attorney General Prosecution

- State Attorney Generals now have the authority to bring civil actions on behalf of state residents injured by a breach, either to enjoin further violations or to obtain damages on behalf of residents
- Total damages imposed on a person or organization for all violations of an identical requirement in a calendar year may not exceed $25,000
- The court may award the costs of the lawsuit and reasonable attorney's fees to the state
- State Attorney Generals may not sue over a specific violation while an HHS action regarding that same violation is pending