

TEXAS ASSOCIATION OF COUNTIES HEALTH AND EMPLOYEE BENEFITS POOL HIPAA POLICIES

MAINTAINING THE SECURITY OF PHI IN THE WORKPLACE

Effective Date: March 17, 2003

POLICY

In conducting the operations of the HEBP Plan, HEBP will manage protected health information ("PHI") in a manner that prevents unnecessary or inadvertent access to, use of or disclosure of PHI.

PROCEDURE

- As to all PHI received by HEBP, staff will:
 - Identify the source of PHI and identify the employees who may receive it and use it to perform Plan functions;
 - Ensure that the PHI will be stored in a secure environment;
 - Not disclose PHI to any individuals not necessary to perform the function for which the PHI was obtained.
- All physical files pertaining to HEBP operations will be stored in a locked room. Only designated staff will access to this room.
- If physical records containing PHI are to be destroyed, they will be put in a locked bin that is picked up by a vendor and shredded in a secure manner. Security codes, locks and/or key cards will be changed or re-programmed as necessary when an employee terminates.
- When working on a file that contains PHI, the designated personnel will keep those files secured at all times. If these personnel must leave their office, either at the end of the day or otherwise, the file must be locked in the desk, the office door locked, or the file returned to the secure file room. No files, papers, disks, CD or any other materials containing PHI will be left unsecured at any time.
- Employees with access to computer files containing PHI will utilize password protocols that protect the security of data stored on the network. Computers will not display PHI in a manner or at a time when it would allow for the inadvertent disclosure of PHI, and an employee's computer will never display PHI when the employee is not at the computer.

- Fax machines and printers dedicated for use by HEBP will be located in a secured room accessible only by designated personnel. Printed materials or faxes containing PHI must be physically secured at all times. If copying is required, materials containing PHI must not be left unattended on the copier.
- Any person who erroneously receive a facsimile, e-mail or other correspondence that should have been directed to HEBP will promptly forward the correspondence to designated personnel without reading it, and without disclosing it to anyone else.
- For each routine function that requires HEBP to disclose PHI, ensure that the PHI is transmitted securely to only the intended recipient.