|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SAFEGUARDS FOR PHYSICAL STORAGE & PROCESSING OF PHI | | | | NO. | |
| It is the policy of American Health Enterprises, Inc. and its affiliated entities to maintain reasonable and appropriate administrative / operational, technical and physical safeguards of information and information systems and address the security of records, electronic and paper, while protecting the integrity and privacy of protected health information (PHI).  Administrative safeguards include policies and procedures controlling access to PHI (refer to related policies and procedures regarding minimum necessary standard and prevention of incidental disclosure of PHI). Administrative safeguards employed by this organization also include thorough and documented pre-hiring screening of employees, as well as appropriate post-employment activities (refer to related policies and procedures regarding security / technical safeguards).  Physical safeguards are actively in place to prevent incidental disclosure of PHI, and include the appropriate maintenance and storage of PHI. Doors to medical records departments and areas where data containing PHI is stored must be secured when unoccupied by authorized individuals with access limited to those deemed as included in the minimum necessary. Filing cabinets should be locked in the event the general area cannot be secured and/or access limited. Current hard copies of medical records will be locked, with keys issued to those identified as the minimum necessary. Access will be revoked upon termination of employment and/or transfer to an unauthorized position in the organization. Patients, visitors and families will not be able to access medical records without written authorization and approval (refer to related policies and procedures).  Electronic workstations will be designed to allow for charts and files to be secured when staff leave their desks, and reasonable attempts will be made to maximize the privacy of patient’s information and protect it from public viewing and incidental disclosure (refer to related policies and procedures and security safeguards). Electronic information will be backed up routinely, in accordance with established security policies, and stored in an environmentally maintained setting designed to protect it against loss of data or damage from heat. Electronic information will be backed up and stored for a period of six years minimum. Vendor requiring access to the network to maintain data systems or upgrade software applications will be permitted to do so under a signed business associate agreement.  Records containing PHI will be maintained for a minimum of six years following discharge of the individual from the organization. Those records exceeding that time period will be destroyed via shredding to ensure secure disposal and preserve confidentiality. In the event of a fire or disaster, portable chart racks will be used to remove hard copy medical records from the facility to another secure location off site. | | | | | |
| Approved: | Effective Date: | Revision Date:  3/17 | Change No.: | | Page:  1 of 1 |