HealthWorks

Building **Healthy** Worksites

IT Practices and Procedures

Privacy of personal health information (PHI) is a very important concern to HealthWorks. Data collected either through our HRA, biometric screenings and/or programming constitutes PHI and is protected in accordance with HIPAA and its corresponding Privacy and Security Rules. As a business associate, HealthWorks is also subject to obligations under the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

HealthWorks does not use or disclose PHI except as permitted or required by law to perform requested services on behalf of our business customers, and to carry out our management and administrative duties. To protect the privacy and security of PHI we come into contact with, HealthWorks has implemented the following policies and procedures:

ADMINISTRATIVE SAFEGUARDS

- All HealthWorks employees are bound by contract to protect and maintain the confidentiality of PHI and other confidential information obtained from our business customers and are required to sign HIPAA confidentiality paperwork.
- No PHI is ever removed from company premises except for legitimate business purposes and unless following appropriate department procedures.
- All employees have unique user IDs and passwords for proper authentication when using the company's electronic systems.
- Employees are required to adhere to the HealthWorks Password Policy
- Employees departing the company have their access rights to the HealthWorks facility and network systems surrendered prior to or simultaneously with their departure.

PHYSICAL SAFEGUARDS & PROCESSING PROCEDURES

- Access to confidential processing data is restricted to authorized processing staff only.
- Data is stored on a secure hard drive accessible only when in the office – except for key company officers who have remote access. Data is backed up daily.
- Personal reports are printed and placed in a windowed envelope clearly indicating the participant's name and address (address is included only if being mailed to individual homes or requested by client) to reduce the possibility of a personal report being sent to the wrong person.
- HealthWorks contracts with an insured document destruction company to destroy sensitive documents. All shredding is done on-site and visible by a HealthWorks staff member.
- PHI is transferred either over the internet via our secure email host, RPost, or directly into our secure portal with a unique login and password assigned to each client. However, only aggregate data is ever shared with our clients.
- HealthWorks uses industry-standard firewall protections.
- Data backups are performed throughout the business day, and are encrypted and moved offsite nightly. Complete data duplication is available at one of our backup data centers, enabling the reconstruction of the entire service within 1-2 business days.

CYBER SECURITY INSURANCE POLICY – a copy of HealthWorks' policy is available upon request.