Privacy and Security Policy

Protecting your privacy and personal information is a priority for HMS Employer Solutions (HMS). Our experience in dealing with sensitive information has allowed us to develop a comprehensive privacy and security policy. Our processes fully comply, and often exceed, the privacy and security mandates set forth by the Health Insurance Portability and Accountability Act (**HIPAA**), Employee Retirement Income Security Act (**ERISA**), and the Federal Trade Commission (**FTC**). We are committed to keeping sensitive information secure.

Information Collection and Retention

We only collect the information necessary to complete our audits. Any superfluous information is removed from our systems and destroyed. As a general rule, the transfer of Social Security numbers from the employer is prevented by the use of an internal employee identifier. In the event that an employer does not have an appropriate internal employee identifier, the use of Social Security number is restricted to data processing only. This data is not available in our application; call center employees and auditors do not have access to this information. All documents received are immediately scanned and stored securely. Access to physical documents is restricted. All documents will be securely stored by HMS for the time period defined by each audit. Upon expiration of the retention period, the documents and any scanned images will be confidentially and securely destroyed onsite by bonded and insured data destruction professionals. A Certificate of Destruction will be provided to the employer.

Information Technology Security

HMS's computer systems are regulated and secured to meet the exacting standards that are needed to handle sensitive data. Our systems are protected from external attacks by a state of the art firewall and segmented computer networks. HMS's systems contain password policies that ensure passwords are complex enough to be secure, and that they are changed often. Laptops are not used for dependent audits; access to data is restricted to specific users on our internal servers. Backups of our data are kept in an access-controlled vault offsite with a bonded and insured data storage company. Any electronic communication of sensitive data utilizes the Secure Sockets Layer (SSL) Protocol, the same technology used by many commercial banks. Our IT professionals regularly audit our system logs for any unauthorized use of our systems. In addition, individual workstations used by call center representatives and auditors have restricted capabilities. These workstations are unable to print, send external e-mail or view external websites.

Physical Security

HMS controls its physical environment with badge entry systems. These systems allow us to only grant access to the areas of the building that are relevant to each employee's position. Our physical security is also enhanced by alarm systems, surveillance cameras, and other methods which cannot be disclosed.

Employee Security

All HMS employees undergo extensive background checks prior to joining our team. Each employee also receives ongoing training and supervision to ensure that he/she is complying with HMS's Security and Privacy Policy.

If you have any questions regarding this policy, please contact us at 1-877-382-4919

As of: March 1, 2012