The HIPAA Security Rule

HIPAA

The Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA is legislation enacted by the federal government to:

- Ensure health insurance portability
- Reduce health care fraud and abuse
- Protect the privacy and confidentiality of health information
- Simplify the administration of health care systems

The HIPAA Privacy and Security Rules apply to covered entities and business associates, which include contracted sales agents and brokers.

Covered entities such as health plans, health care clearinghouses and health care providers who engage in electronic transactions must follow HIPAA Regulations.

The HIPAA Security Rule

The Security Rule mandates any health plans, health care clearinghouses, and any health care providers that manage patients' electronic Protected Health Information, ePHI, to implement proper safeguards to protect the patients' ePHI.

This includes protection of individuals' electronic personal health information that is created, received, used, or maintained by a covered entity such as HealthSpring. It allows these authorized parties to share PHI for the purposes of patients' health care treatment.

As a covered entity, HealthSpring, has put administrative, physical, and technical safeguards in place to ensure our customers' electronic PHI remains confidential, uncompromised, and secure.

Always be mindful and careful of **PHI-related documents**. These can include:

- Electronic storage
- Transmission
- Media devices
- Hard copies

Also be mindful of where and how you discuss PHI-related documents no matter which format. Someone could overhear your conversation.

HealthSpring℠

Technology Do's

- Do verify a FAX number with the recipient prior to sending information and verify post-transmission that the information was received
- Do secure your wireless connection before transmitting PHI wirelessly via the Internet

Technology Dont's

- Do not reveal or share your user IDs and/or passwords with anyone
- Do not browse or use CMS data files for unauthorized or illegal purposes, for private gain, or to misrepresent yourself or CMS
- Do not allow unauthorized access to fax machines that are used to transmit PHI and always confirm you entered the correct fax number before sending
- Do not store PHI on your phone or any other portable devices (iPad, etc.)
- Do not share or duplicate unauthorized CMS data
- Do not email completed enrollment forms or protected information without using a secure or encrypted email transmission

Health Information Technology for Economic and Clinical Health (HITECH)

The Health Information Technology for Economic and Clinical Health, or HITECH Act, is a law that promotes adaptation and meaningful use of health information technology.

HIPAA's enforcement rules were strengthened by the HITECH Act by:

- Improving privacy and security provisions in the original HIPAA Privacy and Security rules
- Making business associates of covered entities directly accountable for compliance with certain HIPAA Privacy and Security Rules
- Incorporating and increasing the civil monetary penalty structure for violations and requiring notification to individuals and the Department of Health and Human Services (HHS), in the case of an unauthorized disclosure of PHI or access to electronic PHI.

HealthSpring℠