

Compliance CORNER

Protected Health Information

In this issues of the newsletter, I'm going to focus on something many of us work with on a daily basis: Protected Health Information (PHI)... and PHI, it just so happens, begins with another acronym near and dear to us all – HIPAA.

As we've all learned in our Annual Compliance Training, HIPAA – the Health Insurance Portability and Accountability Act – seeks to safeguard patients from the improper use or disclosure of their information once it is given to healthcare providers. Within the context of HIPAA, PHI is defined as information that is created or received by a Health Plan, Healthcare Provider, or Healthcare Clearinghouse, and relates to an individual's health, provision of care, or payment for care, and identifies the individual. As an entity covered by HIPAA, when we receive a patient's PHI, we are responsible for safeguarding the information when we obtain it, store it, access it, transfer it, or destroy it.

PHI can be in many formats, including electronic, paper, and verbal. PHI includes the following 18 items under HIPAA Privacy Rules:

- Patient Name
- All geographic sub-divisions smaller than a state (street address, city, county, precinct, zip code, and equivalent geocities)

- All elements of dates except year (birth date, admission date, discharge date, date of death, date of service)
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and county, precinct, zip code and equivalent geocities
- Device identifier's serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voiceprints
- Full facial photographic images and any comparable images
- Any other unique number, characteristic, or code

Entities covered by HIPAA cannot share a patient's PHI without his/her permission unless it is for Treatment, Payment, or healthcare Operations (TPO). This means patients must give their written authorization allowing the use of their PHI for any reason outside the scope of TPO. Each patient receives a formal "Privacy Notice" from ARS, which informs the patient of how their PHI will be used and advises them of their rights under HIPAA. HIPAA also requires that covered entities limit their PHI to the "minimum necessary" to accomplish the intended use.

In summary, use common sense and discretion when discussing, transmitting, storing, and disposing PHI. If PHI is treated with care and responsibility, both patients and providers are protected.

If you have any questions regarding HIPAA or PHI, you can contact either Amanda Eagan, our Privacy Officer, or me.

**GOOD COMPLIANCE IS
GOOD BUSINESS!**

By: Scott Poblenz, Corporate Compliance Officer

