HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT OF 1996 (HIPAA)

Prior to the HIPAA privacy rule, your personal health information could be used by hospitals, pharmaceutical companies and brokers for marketing purposes. There was no strict mandate that employers who had access to your private health information couldn't use the information for adverse personnel actions in employment. Most employees do not want their medical history released to their supervisors and co-workers.

The HIPAA privacy rules and regulations were mandated to begin 14 April 2003. The privacy rule, for the first time, created national standards to protect individuals' medical records and other personal health information (PHI). It sets boundaries on the use and release of health records. It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information. It holds violators accountable, with civil and criminal penalties that can be imposed, if they violate privacy rights. HIPAA has privacy rules that affect everyone in the workplace.

PHI is used when it is shared, examined, applied, and analyzed. PHI is disclosed when it is released, transferred, or accessed by anyone outside the NAF health benefits plan and NAF authorized employees. Anytime PHI is used outside of treatment, payment, and health care operation (TPO), authorized employees must obtain a signed authorization form from the individual before releasing only the requested information.

Ways to secure PHI: (1) Lock your computer station when you are not physically at your desk, (2) Do not leave voicemail messages with PHI, (3) Do not receive faxes containing PHI in public areas without monitoring receipt of the fax, (4) Shred documents containing PHI before disposing of them, (5) Lock cabinets containing PHI, (6) Use minimal necessary standard when transmitting PHI through e-mail for treatment, payment, and health care operation purposes, (7) Do not leave papers or electronic memory devices with PHI unattended or unsecure on your workstation, (8) Remove unique PHI identifiers (names, social security numbers, e-mail addresses, date of birth, license plate numbers, and any unique characteristics or codes) which will link an individual to his or her health information, (9) Destroy any documents containing PHI that are no longer needed, and (10) Do not discuss PHI over the phone if non-authorized employees are present.

Failure to comply with the HIPAA privacy rules can result in a fine of up to $100 per incident, and up to $25,000 per person, per year. Criminal penalties will apply if a person knowingly discloses PHI and/or misuses a unique health identifier. Knowingly disclosing information can incur up to $50,000 in fines and one year in prison.

Obtaining information under false pretenses can result in up to $100,000 in fines and five years in prison.

Even if you are not a supervisor, protection of PHI is everyone’s responsibility. If you must refer to a co-worker’s health, use non-specific terms like “relapse, setback, or serious medical condition”. Treat their information as discreetly as you’d like them to treat yours.

I have read and understand the HIPAA guidelines outlined above and I understand that this applies to me.