

The first few days on the job are critical. Your colleagues' initial assessments and observations of you typically turn into long-term perceptions and reputations. You learn quickly that your co-workers will only take you as seriously as you take yourself—and your work.

By maintaining a positive attitude, colleagues will find you friendly and more approachable, and you'll make a positive, lasting impression.



Follow these simple suggestions for making a great first impression:

- **Work full days:** Arrive to work early and stay late. This shows that you are motivated and dedicated.
- **Stay on top of your duties and responsibilities.** Establish your priorities by setting challenging, but achievable short-term and long-term goals.
- **Listen more than talk on those first few days.** You don't want to seem like a know-it-all.
- **Maintain a pleasant demeanor** Dress professionally and keep your boss informed of your work progress.
- **Avoid gossiping and bad-mouthing your colleagues or boss.** This can tarnish your reputation, which is difficult to repair.
- **Should your reputation become damaged, apologize to co-workers.** Let them know you will work hard to improve your relationship.
- **Take advantage of out-of-work activities, such as sports leagues or an employees' activities committee.** This is also a great way to bond with co-workers.
- **Meet and network with key people in the organization.**
- **Attend staff conferences and seminars to further your knowledge of the field.**

Compliance Corner

Answering your Compliance, Coding, HIPAA Privacy and Security Questions



Fellow Employees,

In this issue we would like to discuss the recently enacted **red flags rule**. Red flag means a pattern, practice or specific activity that indicates the possible existence of identity theft. Identity theft is defined as fraud committed using the identifying information of another person. News reports of identity theft are increasing, and now not only is there concern about theft of financial information but also medical (insurance or payor) information. Medical identity theft is defined as stealing a patient's insurance information and using it to obtain and pay for medical care.

It is our responsibility to protect every patient's right to privacy of their protected health information. This is accomplished by following policies regarding release of information (HIPAA policies) and now the new red flags rule. This new regulation will be enforced by the Federal Trade Commission and requires institutions with patient accounts to design a program that will

detect, prevent and mitigate identity theft. Health care providers that maintain patient accounts must comply with this new regulation.

Types of red flags:

- Suspicious documents
 - Suspicious personal identifying information
 - Suspicious or unusual use of a patient account
 - Alerts from others (e.g., customer, identity theft victim or law enforcement)
 - Treatment or physical exam that is inconsistent with documentation in the medical record from a previous admission.
- Items to consider include: blood type, age, race and other physical descriptions that may be evidence of medical identity theft.

All potential red flags must be reported to a manager or supervisor to investigate as appropriate. Managers and supervisors must report all confirmed issues to compliance. All staff is also

continued on page 10