# Health Information Compliance Alert

## Action Plan: 9 Pointers Help You Reduce ID Theft Potential

**Vigilance holds the key to prevention.**

**Facility challenge:** Because of patient numbers and the higher potential that facilities won't have prior relationships with patients, "it is not physically possible for hospitals and specialty practices to prevent medical ID theft entirely," warns **Ester Horowitz, CMC, CITRMS, CIISA.** Good faith efforts to put in place compliance plans will reduce it and slow it down.

Read on for field-tested tips on closing the gap on security breaches in your practice:

1. Ensure patient authentication before providing service. Primary care practices and small practices have an opportunity to develop interpersonal relationships with their patients in a way that they can be a little more suspicious about people who claim to be something they are not, Horowitz adds. For example in a pediatric practice someone posing as an aunt, grandmother or family friend of a child needs to be questioned. In the case of internal medicine, checking for family and close relationships on the primary history would be helpful with new patients. The insistence upon certain drugs or the need for more than what is being prescribed is another indication.

Your best firewall is your front desk protocol, experts say. Many providers will scan the driver's license of an individual into their records when providing services or information, or require additional identification warns **Jim Sheldon-Dean**, Director of Compliance Services, Lewis Creek Systems, LLC in Charlotte, Vt. "Use the scanned information as part of the encounter process to verify individuals relative to past information. Mismatches of information between government-issued ID and health insurance cards can be a tip-off," he advises.

2. Lock out portable devices. "Make sure that all personal belongings are not allowed in the work area such as cell phones or USB thumb drives," says **Barbara J. Cobuzzi, MBA, CPC, CENTC, CPCH, CPCP, CPC-I, CHCC,** president of CRN Healthcare Solutions, Tinton Falls, N.J. "A secure operation will make sure that employees leave all personal belongings outside the work area so that there cannot be a data breach," she warns.

A phone can take a picture of a computer screen and a thumb drive can copy data off a system. So, even in a paperless environment, these electronic devices that are included in the workers' personal belongings need to be considered and barred from the workplace, Cobuzzi adds.

3. Divide up data protection duties. Breaking up authority among many rather than allowing one person to have too much authority will also reduce medical ID theft and any kind of fraud for that matter, suggests Horowitz.

4. Lock up script pads and don't leave them unattended in the presence of patients. Another deterrent is not allowing staff to have easy access to them, says Horowitz.

5. Hire very carefully. Make sure you hire people who have demonstrated good character, says Horowitz. Background checks are a good way to do that.

6. Background checks should be made of vendors as well. An inside job sometimes includes more than one person performing the illegal act, warns Horowitz. Passing information to vendors would be an excellent way. Ensure that there are no personal relationships between vendors and staff, she says.

For example, if a staff member recommends someone they know to become a vendor, examine the relationship, she recommends. Does the staff member receive a referral fee? Does the staff member have an interpersonal relationship? Many organizations like to work with people they know well because they want to trust them, but it would be prudent to perform background checks even on trusted recommendations to flush out potential conflicts of interests that weren't brought forward in the spirit of transparency, adds Horowitz.

7. Conduct regular system checks. "Adopt an information security management process that involves regular reviews and evaluations to ensure your measures are as effective as they can reasonably be, and fully documents your actions, activities, and assessments undertaken in compliance with your policies so you can be ready to deal with any issues or external audits that arise," says Sheldon-Dean.

8. Conduct unannounced audits. To reduce the incidence of ID theft, a surprise audit of compliance practices is a good tool. Letting staff members know that such audits can occur at any time is a deterrent to committing theft and fraud.

9. Be vigilant about educating staff. Educating staff is considered the second most important thing you can do and it is also a requirement in the compliance process, says Horowitz. There is not enough education being performed or made easily available.