Medical Identity Theft

Medical identity theft is a growing concern for individuals and employers. More than 1.8 million Americans became victims of medical identity theft in 2013, with an average loss of more than $22,000 per incident, which is six times higher than the average loss due to financial identity theft. Employers are negatively affected through lost employee productivity and through the fraudulent overuse of health plan benefits.

What Is Medical Identity Theft?
Medical identity theft occurs when someone uses another individual’s personal information, which may include his or her name, birthdate, Social Security number and insurance information, to obtain medical services, devices or prescriptions. Medical identity theft is a serious crime that can lead to both financial loss and harmful inaccuracies in the victim’s medical records and health benefits claims.

The Harm of Medical Identity Theft
The financial impact of medical identity theft can include lost money, unpaid bills and collection agency letters, and tarnished credit reports. Finding and correcting records can be a lengthy process, often taking as long as a year to complete. The messy consequences of inaccurate medical records and insurance claims can be both a time-consuming nuisance as well as a threat to the victim’s health. The medical repercussions for medical identity theft victims can include misdiagnosis, conflicting prescriptions, missed symptoms and other harmful consequences.

Medical identity theft, aside from hurting and distracting your employees, will affect your company. Employee productivity will likely decrease while the victimized employee works through the time-consuming process of correcting records, recovering money and contacting authorities. The thief may also have initiated false benefits claims, impacting your benefits costs. How the false claims affect you will vary, but medical identity theft can be especially costly for employers with self-funded plans.

Where Do Threats Come From?
Threats to medical identity security can come from several different sources:

• **Friendly** – “Friendly fraud” occurs when a friend or family member illegitimately uses another person’s identity and medical information to obtain health care services or goods. Studies estimate that somewhere between one-third and one-half of all medical identity theft is committed by a friend or family member.

Friendly theft may include an employee handing over an insurance card or plan number in an attempt to help a friend in need, or it may result from the unauthorized use of a family member or friend’s name and insurance information.

• **Providers** – Dishonest staff in providers’ offices, including nurses, doctors, technicians, receptionists or other individuals, can steal private information. Identity thieves can either sell the information to those who will then assume the victim’s identity in order to obtain medical goods or services, or the information can be used to scam insurance companies into paying out false claims.

• **Hackers** – Personal and medical information can be bought online by someone who wants to use another person’s identity to obtain medical services. In addition, the increase in electronic health records (EHRs) is presenting greater opportunity for...
criminals to illegally access private information. According to information from the Department of Health and Human Services (HHS), breaches in medical information security have affected more than 31 million Americans in the past five years.

How to Prevent Medical Identity Theft
Preventing medical identity theft is difficult. Aside from keeping information as secure as possible, the best defense is for individuals to be vigilant and to carefully review their bills, medical records and insurance information for any fraudulent activity.

Although not completely preventable, early detection of theft will contain the amount of damage and help speed the recovery process. Here are some tips to share with your employees:

- Use strong, unique usernames and passwords.
- Don’t share personal information, and don’t give medical insurance cards or information to family or friends.
- Keep all medical records in a safe place, out of view of visitors in the home.
- When disposing of records that no longer need to be kept, shred them before recycling.
- Always carefully review the explanation of benefits (EOB) letters, medical bills and any other medical records received; look for any services or medications you did not receive or for inaccurate medical information.