

Health Information Compliance Alert

Health Information News

PROTECT PHI FROM YOUR STAFF

Your best intentions can be easily thwarted by employees intent on grabbing your patients' PHI.

That's the lesson two providers learned after staff members stole detailed financial information - including Social Security and account numbers and birth dates - from the records of more than 100 patients.

Tiana Hill, an employee in the University of Chicago Physicians' Group billing department, and **Bonnie Williams**, a receptionist at Lincoln Park Family Physicians, were arrested for allegedly supplying patient information to an identity-theft ring that involved 10 other people and netted the criminals \$150,000, the Chicago Sun-Times reports.

Both medical groups have made sweeping reforms to the way they protect patients' records.

The Bottom Line: Act now to identify and deal with suspicious behavior before a crime is committed.

WATCH OUT FOR EX-EMPLOYEES

An angry, vindictive employee could be your worst enemy when it comes to protecting patients' PHI.

Joseph Nathaniel Harris, a former branch manager of the San Jose Medical Group, was charged with the March 28 theft of computers and a disk that contained a database of patient records.

Federal agents honed in on Harris after connecting the crime at San Jose Medical Group to one weeks earlier at the Silicon Valley Children's Fund. Computers stolen from the entities wound up listed on a second-hand sales Web site under an e-mail address linked to Harris.

Harris was fired from the San Jose Medical Group after being accused of stealing money and medication; he was fired from the Silicon Valley Children's Fund for focusing too much energy on his side business - computer sales.

The Bottom Line: Tight security measures such as encryption or password protection can help you avert any employee's harmful intent - and save both your compliance and your patients' identities.

HERE'S HOW TO GET YOUR ID

Pay attention to differing effective dates for your three national provider identifier (NPI) application method choices to ensure your submission process runs smoothly.

Important: You can choose one of the these application methods:

1. Apply online at <https://nppes.cms.hhs.gov> beginning May 23.
2. Mail in a paper application form beginning July 1.
3. Submit your application, together with other providers' applications, beginning in the fall of 2005.

The Bottom Line: Apply for your NPI using only one of these methods after CMS' specified dates. For more information, go to www.cms.hhs.gov/medlearn/matters/mmarticles/2005/SE0528.pdf.

YOUR PATIENTS ARE PUSHING FOR EMRs

While you may be hesitant to begin the transition to electronic medical records (EMRs), your patients could be leading the pack.

Almost 10,000 patients have signed up for a free service that allows them to piece together their own medical records and access them from anywhere through the Internet.

Developed by Medem Inc., a nonprofit organization formed by the American Medical Association and six other medical associations, iHealthRecord is a subscription-based service that is protected by encrypted security features similar to those in the financial services industry. About 100 doctors subscribe to the site.

Bonus: The service updates subscribers about medical research and notifies them by e-mail if the U.S. Food and Drug Administration issues new or altered information about any prescribed medication.

The Bottom Line: The federal government is encouraging private practices to transition to EMRs, but it may be patients' demand for comprehensive, interactive records that pushes the industry closer to its goal.