Medical Practice Compliance
News, tools and best practices to assess risk and protect physicians
ALERT
June 10, 2013 | Vol. 25, Issue 11

Take 7 steps to protect your practice's NPI, DEA numbers

by **Marla Durben Hirsch**

It's hard enough to protect your patients' confidential information from security breaches. But an unauthorized use of your National Provider Identifier (NPI), Drug Enforcement Administration (DEA) or other provider number exposes you not only to identity theft but also billing fraud and criminal investigation. That's what happened to a Sacred Heart Hospital provider in Chicago. Kenneth Nave, M.D., was arrested for using another physician's DEA number to write more than 100 prescriptions for hydrocodone to patients at the hospital. He used the ruse that he was filling in for the physician whose number he stole while he or she was out "sick," according to FBI affidavits obtained by *MPCA.* It's not yet known whether the "sick" doctor was a victim or willing participant in Nave's scheme, but the investigation also uncovered fraudulent billing and is ongoing, says Randall Samborn, spokesperson for the U.S. Attorney's Office in Chicago.

Once stolen, a physician's ID can amass millions of dollars in unauthorized claims or hundreds of bogus prescriptions before anyone's the wiser, warns Sam Imandoust, CPA, Identity Theft Resource Center in San Diego. DEA number misuse is rampant because of a national epidemic of controlled substance abuse, which triggers scrutiny of prescription misuse, notes attorney Colbey Reagan with the Waller law firm in Nashville.

At best, a physician ID theft victim has to deal with a government investigation to rule him or her out as a suspect. That can have "severe" financial and reputational affects, Imandoust warns. Also, CMS may cease payments to the physician during the investigation.

But if you shared or lent your numbers to someone else, even naively or in good faith, you can be found liable for billing fraud or violations of the Controlled Substances Act — a criminal offense — or be stripped of your license or DEA privileges, warns Susan Miller, co-chair for the Workgroup for Electronic Data Interchange's (WEDI's) security and privacy workgroup in Reston, Va. And if patients' information was compromised in the process, you can face HIPAA violations, Miller warns.

3 ways your medical IDs are at risk

Providers' national provider identifiers (NPIs) and Drug Enforcement Administration (DEA) numbers are easy prey for ID thieves. Here's how:

- NPIs are publicly available on the National Plan and Provider Enumeration System (NPPES).
- DEA numbers are listed on every page of a physician's prescription pad.
- Both the NPI and DEA numbers can be found in electronic health records, which are vulnerable to snooping by rogue employees and cyberattacks, says attorney and legal analyst Sam Imandoust, CPA, for Identity Theft Resource Center in San Diego.

Continued on following page

7 tips to safeguard provider numbers

"It can be overwhelming [to secure your provider numbers] and physicians may have higher priority things going on, like the patient in front of them," Imandoust says. But it pays to be proactive.

Use the following to tips to protect your data:

- **Share your NPI sparingly**, Miller says. A few arrangements do require physicians to lend or share their NPIs, such as reassignment. In those cases, validate who will use it and for what purpose, Reagan says.
- **Safeguard your DEA number by locking up prescription pads.** Use pads with watermarks because they're harder to replicate and inventory pads regularly, Reagan suggests.
- **Check the OIG's exclusions database to vet NPI numbers of new hires and physician partners** — even if you're a small practice. Check that they are valid and they haven't been excluded from federal health programs, says Imandoust.
- **Monitor remittance advices, claims and reimbursements to verify billed services match your income**, Imandoust says. That will let you know if someone is diverting your reimbursements to a bogus address.
- **Check your credit report for unusual behavior under your name.** If your NPI or DEA number has been compromised, your personal data, such as your name and address needed to open a line of credit, can also be affected Imandoust explains.
- **Review your enrollment information with payers** to make sure that it's correct and nothing has changed, Imandoust suggests. Know whether your address was changed without your authorization.
- **Notify CMS and the DEA if you believe your NPI or DEA number was compromised.** CMS created a formal initiative program for physicians that had their NPIs misused for fraudulent billing. Report suspected Medicare ID theft — only if haven't yet incurred financial liability — to your Medicare administrative contractor (MAC) or the Office of Inspector General (OIG). Visit *www.dea.gov* for how to file a report if your DEA number was compromised.

This article originally appeared in Medical Practice Compliance Alert, a publication of DecisionHealth, and is reprinted with permission. For more information of Medical Practice Compliance Alert or to buy a subscription, visit www.decisionhealth.com/mca