Codify
BY AAPC

Part B Insider (Multispecialty) Coding Alert

Privacy: 8 Steps to Take Right Now to Avoid Medical Identity Theft

Beneficiaries aren't the only potential victims of this problem.

As a medical professional, you're probably acutely aware of how quickly a Medicare beneficiary can become the victim of identity theft—if they leave their Medicare card in the wrong place just once, they can have their identity stolen, leading to scores of problems. But did you know that thieves are also itching to get their hands on your billing numbers as well?

That's the word from CMS's training course, "Safeguarding Your Medical Identity," which the agency recently updated with new information on how to prevent becoming victims of this growing trend.

Know What's At Risk

"Medical identity theft is the inappropriate or misuse of a patient's or physician's unique medical identifying information to obtain or bill public or private payers for fraudulent medical goods or services," said **Shantanu Agrawal, MD,** a medical director with CMS, during the presentation. In 2009 alone, over 3,600 physician and patient cases of medical identity theft were reported. Unfortunately, that number is continually creeping higher, he added. Currently, the government is tracking about 5,000 compromised provider identifiers (such as NPIs) and about 280,000 compromised beneficiary identifiers (such as patient ID numbers).

To make sure you aren't next in line for medical thieves, follow these eight steps that will help keep your information safeguarded.

1. IRS Notices Reveal More Than You Think. If your identity is stolen, that income is reported to the IRS—and the feds will eventually wonder why you aren't paying taxes on it. Therefore, pay attention to any notifications that the IRS sends—they could alert you to fraudulent activity that's taking place with your Medicare number. One physician had to pay an attorney $600 per hour over a four to five month period to clear her name after her Medicare billing numbers were stolen—by the time the operation was shut down, the company that stole her identity was found to have tried to launder up to $4.7 million under 19 doctors' names. This can happen to doctors, nurses, NPs, Pas and other medical professionals, Agrawal said.

2. Keep Track of Prescription Pads. "Anyone can walk away with them if they are left in the open," Agrawal noted. You should also use tamper-resistant prescription pads, which Medicaid has required since 2008. These must include a watermark or thermal ink, which show attempts to alter prescriptions. Even so, however, these methods are not foolproof, he adds, so always take every precaution by locking up prescription pads when not in use.

3. Activate Computer Log-ons. "Disabling log-ons is a dangerous practice, and sometimes people do it to make life a little easier and access quicker for employees," Agrawal said. However, these steps are essential to keeping the information on the computer safe. Each staff member should have a unique log-on code, and if an employee leaves the practice, remove his or her log-on access immediately so they can't get into the system.

4. Actively Manage Enrollment Information With Your Payers: "Physicians can actively manage enrollment information with payers by updating them about material enrollment changes, especially when opening, closing or moving practice locations, or when separating from an organization," Agrawal said. This way, if a payer receives claims or reimbursement requests to an old or non-existent office location, they can contact you and ask about it.

5. Monitor Billing And Compliance Processes: "By strengthening compliance activities, physicians can minimize risk and improve their overall program integrity," Agrawal said. "Physicians must be aware of billings in their names, paying close attention to the organizations and mid-level providers to whom they have assigned privileges." In addition,

compare remittance notices with medical record documentation and ensure that mid-level practitioners' documentation supports billed services. Read all items before signing them, keep copies, and document conversations about billing issues. "Remember, whether staff or a third party biller provides the organization's claims processing services, the physician of record is responsible for the claims submitted," he said. "Once a physician has signed off and claims are submitted, the physician is certifying to the truth and accuracy of them."

6. Pay Attention to Patient Complaints. Listen when a patient tells you he started receiving medical items that he never ordered, says **Julie Taitsman, MD,** chief medical officer at the OIG, during the course. It's possible that someone is ordering the items in the patient's name or maybe even with your provider number to collect reimbursement they don't deserve.

7. Avoid Sharing When Possible. Even doctors doing things correctly are still at risk for medical identity theft, Taitsman said. One big risk factor is when doctors have given their identifying numbers to high numbers of other entities, such as giving your TINs and NPIs to various clinics, hospitals, doctors and mid-level providers.

8. Report Potential Issues to the Police. One doctor reported that her medical identity was stolen and was later used to submit fraudulent claims to government payers. She initially waited for the Medicare system to correct it, but later found out that any type of medical theft□including medical□should actually be reported to the police department.