

## Preventing Identity Theft: What You Need to Do

Samuel A. Collins

Q: I understand that there are some new rules regarding identity theft that will be implemented this year. Is there something I must do to comply with these rules or am I exempt because I am an chiropractor and most of my patients pay cash?

A: You are correct that there will be further implementation of [HIPAA regulations](#), under the direction of the [Federal Trade Commission](#), to protect patient privacy of their health information. Specifically, this new rule, referred to as the "red flags" rule, covers identity theft. Providers of health care services must implement a protocol to prevent identity theft and identify patterns or practices that may indicate potential identity theft. [To learn more about the rule, implementation of which has been delayed until later this year, read "[Are You Ready for the Red Flags Rule?](#)" in the July 1 issue of *DC*.]

Essentially, the rule is designed to prevent someone from using another person's name or identifying information to submit invoices, statements, bills, insurance billing or for other purposes consistent with collection and reimbursement of health care services. Therefore, any provider who bills for services, even simple cash transactions, will need to follow the new regulations to prevent identity theft.

It has been misconstrued that privacy regulations do not apply if you do not bill insurance or bill electronically. In fact, privacy rules do apply to all providers - all patients have a right to the privacy of their medical information, so all health care providers have a duty to ensure the protection of that information. However, the level of standards and procedures required in each office can vary greatly. Certainly if you are not doing electronic billing, the privacy regulations pertaining to electronic data need not be followed. However, just because you may not do that particular type of billing does not exempt you from the overall rules of privacy.

Don't feel intimidated by this. It simply requires that you have a written protocol outlining what your office does to recognize and prevent identity theft; more specifically medical identity theft. The following is a simple format for a document of compliance that could be titled "Detecting Red Flags of Identity Theft." This example is for a small health care practice with a well-known, limited patient base and a low, minimal or nonexistent risk of identity theft. The following procedures should be followed to identify red flags:

- All prospective new patients are required to establish their identity by producing an unexpired driver license or state identification card with a photograph. The license or identification card is examined to determine whether it is current and appears to be valid. Specific holograms and other markings are examined for authenticity. A photocopy of the license or card is made and kept on file. The absence of these features indicates that the license or identification card is counterfeit.
- The name and address information on the driver license or identification card is compared to the address on the insurance information furnished by the new patient. Any discrepancies must be

resolved.

- The name and address information on the driver license or identification card is compared to any credit card or bank check produced for payment of services. Any discrepancies must be resolved before accepting payment.
- Prospective patients are requested to fully complete intake forms and produce for photocopying insurance cards or other proof of insurance. The information on the completed intake form, insurance card or other proof of insurance is compared with the driver license or identification card. Any discrepancy must be resolved.
- The prospective patient is not accepted as a new patient until all of the aforementioned discrepancies are resolved.
- All staff are trained to follow the above-listed identification and detection factors.

The above is essentially all that is needed, as it serves as a written protocol for compliance with the new regulation. For the most part, this is likely something you were already doing as part of your practice; now you are documenting the protocol in writing. If you'd like more information, I will send a complete compliance document for this regulation that includes more detail, as well as specific follow-up protocols when there may be a discrepancy. Please contact me at [sam@hjrossnetwork.com](mailto:sam@hjrossnetwork.com) and request the "identity theft" document in the subject line.

SEPTEMBER 2009