# Health Law Bulletin

provided by:

MITCHELL • BLACKSTOCK

Mitchell • Blackstock • Barnes • Wagoner • Ivers • Sneddon • PLLC

## What To Do If Financial Or Medical Information Is Stolen From Your Practice

A theft of financial, personal or medical information from your practice creates duties on you to take certain steps to notify and protect your patients from identity theft. Theft of electronically stored information is covered by Arkansas law, as well as federal law.

The theft of paper documents, such as credit card receipts, checks, superbills or patient charts, does not carry with it exactly the same reporting requirements as the theft of electronically stored data. Nevertheless, the theft of any kind of information from your practice should be reported to your patients.

The obvious first step is to call the local police to report the theft and to do all you can to cooperate with them. Unfortunately, it is not uncommon that the culprit is someone employed by the medical practice or someone who has some legitimate access to the premises. Your two defenses against this kind of theft are: (1) proper hiring practices not only for your daytime staff but for auxiliary services such as cleaning and (2) practices that limit access to money, superbills, other medical records, to laptops, and to information in your computer system. You also can consider after-hours video surveillance of certain areas.

You will have to determine what is missing and then create a list of the *types of information* that is at risk. For example, were bills taken that contained medical diagnosis information, financial information, and insurance information? Were Social Security numbers on any documents? Was the information on paper or did it come from a breach of the computer system? Were laptops stolen that contained patient information? For electronically stored information, you will need to determine whether it was encrypted.

The best response to a theft of information is to promptly notify the patients who were affected, but before doing so, you will want to visit with your legal counsel on what laws apply to your particular situation. Be aware that certain timelines may apply, and in any case, you should act quickly to let your patients know that they should monitor their financial and medical statements. Thieves may be using the stolen information or documents to open new credit accounts, to steal money from your patient's financial accounts, or for medical identity theft in which a person assumes the identity of your patient in order to obtain healthcare covered by insurance or as part of a fraudulent Medicare/Medicaid billing scheme. If documents were taken that show the physician's Medicare/Medicaid provider number, more sophisticated thieves may

use that number as part of a Medicare/Medicaid fraud scheme in which someone pretends to be the physician and bills for services never provided.

You are no doubt familiar with the Red Flag Rules, which deal with identity theft. The implementation date of these rules for physician's offices has been postponed three times because the American Medical Association has objected to their application to physicians. Nevertheless, the current implementation date for physician's offices is November 1, 2009. The Red Flag Rules set out what must be contained in any notice of a security breach. Likewise, the Arkansas Personal Information Protection Act has its own requirements for disclosure of personal information via a breach of a computer system. Finally, the amendments to HIPAA that were passed earlier this year have specific notification requirements that must be followed in the event of a breach of protected health information. The nature and extent of the notification depends on the number of patients potentially affected by the breach.

It is impossible to stop all theft all of the time. Physicians' offices should be aware of their obligations under federal and state law to properly secure information maintained in an electronic format and should take common sense precautions to limit access to paper medical records and to limit access to cash, credit card information and checks. If a theft does occur, experienced legal counsel can assist you in navigating your obligations under the law.