

# Detering and Remediing Employee Theft

Bill Buzogany\* and Michael J. Mueller†

**E**mployee theft of patient-related information for personal financial gain is a serious threat to the success and financial viability of many healthcare providers. You can safeguard your financial interest in your patient base by taking three preventative measures designed to dissuade your employees from stealing from you. The first step is the implementation of policies and procedures that inform your employees that patient-related information is a valuable business asset that you vigorously protect from misappropriation. The second step is strictly limiting and monitoring employee access to patient-related information. The third step is educating your employees of the potential legal consequences to them in the event they steal from you and, in the event of theft, pursuing all legal remedies available to you.

**Key words:** HIPAA; patient base; theft; deterrence; prevention; remedies.

Your patient base and related information are your most important and valuable assets. Are you protecting them? Your patient base is constantly under siege from competitors, but the greatest threat you face may very well come from within—that is to say, your employees may be seeking to steal your most valuable assets for their own financial benefit.

***HIPAA protects patients from the unauthorized disclosure of information relating to their health—it does not protect you from employee theft of patient information.***

It is all too common today for healthcare employees to steal and then “sell” patient information to competitors, either directly or by holding themselves out as “contractors.” Many healthcare providers believe that HIPAA provides them with adequate protection against employee theft of patient-related information. However, relying upon HIPAA as a safeguard against employee theft of that

information can prove to be a costly mistake. After all, HIPAA is designed to protect *patients* from the unauthorized disclosure of confidential information relating to their health conditions. HIPAA is *not* designed to protect healthcare providers from employee theft of patient information.

***To protect your patient information, have your employees commit in writing that they will not make unauthorized disclosure of patient information, limit and monitor employee access to patient information, and inform your employees of the legal consequences attached to theft of patient information.***

Three steps that you can and should take in order to prevent employee theft of patient information can make all the difference between operating a successful and profitable business and going out of business:

- **Step One:** Deter employee theft by implementing policies and procedures that commit your employees, in writing, to forbear from making the unauthorized disclosure or use of your patient-related information.
- **Step Two:** Prevent employee theft by limiting your employees’ access to your patient-related information.

\*Buzogany Marks & Mueller LLC, 225 West Washington Street, Suite 2200, Chicago, IL 60606; phone: 312-924-2882; fax: 312-268-6473; e-mail: wbuzogany@bmm-law.com. †Buzogany Marks & Mueller LLC; e-mail: mmueller@bmm-law.com; Web site: www.bmm-law.com. Copyright © 2010 by Greenbranch Publishing LLC.

- **Step Three:** Dissuade employees who may be tempted to steal from you by making them aware of the consequences, both civil and criminal, of doing so, and by making it known that you will pursue all available remedies in the event of employee theft of your patient-related information.

## STEP ONE: POLICIES AND PROCEDURES

### Employee Handbooks

If you have an employee handbook, it should contain a provision notifying your employees that in addition to being confidential, patient information is an asset of your business and that the unauthorized review, disclosure, and/or use of that information may result in discipline, up to and including the termination of employment. Your employees should be required to sign an acknowledgment form that states that they have been apprised of your policy regarding the patient information, that they understand and agree to comply with your policy, and that they understand that they may be discharged if they violate the policy. The signed acknowledgment form should be maintained in the employee's personnel file, and employees should periodically be reminded in writing of their obligations regarding patient information. In the event of litigation regarding the theft of patient information, a signed acknowledgment form and reminder statements will constitute valuable evidence for the purpose of establishing that an employee knowingly misappropriated your property and that you are entitled to relief from a court.

### Confidentiality Agreements

You can also require your employees to sign confidentiality agreements, pursuant to which they agree not to make unauthorized disclosure of patient information to others and/or to misuse—either by themselves or in concert with others—patient information. A signed confidentiality agreement should be maintained in the employee's personnel file, and employees who sign such agreements should periodically be reminded in writing of their obligations under the agreement. In a legal proceeding, a confidentiality agreement can serve as valuable evidence for the purpose of establishing that an employee knowingly misappropriated your patient-related information, and that you are entitled to relief from a court.

### Noncompetition Agreements

A noncompetition agreement is a very effective tool you can use to dissuade employee theft (such agreements are generally enforceable in most states; California is a notable exception). Such agreements typically provide that: 1) certain information (such as a patient list) possessed by the employer is confidential and proprietary in nature and has economic value, actual or potential, from not being

generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use; 2) the information is the subject of efforts that are reasonable under the circumstances to maintain its secrecy; 3) the employee, by virtue of his or her employment, has access to the employer's confidential and proprietary information; 4) the unauthorized disclosure and/or misappropriation of the confidential information would cause the employer irreparable harm, entitling the employer to injunctive and other legal relief, such as court costs and attorneys' fees in the event of litigation to enforce the agreement; and 5) the employee agrees not to misuse the confidential information, and not to compete with the employer while employed by the employer and for a certain period of time following the end of the employment relationship.

To be enforceable, agreements not to compete must be reasonable with respect to both duration (generally up to three years following the end of the employment relationship) and geographic scope (generally the area in which the employer does business). A signed noncompetition agreement likely will constitute valuable evidence in your favor in a legal proceeding related to employee theft of patient information, and like other employment-related documents should be maintained in the employee's personnel file.

### Moonlighting

Employees with multiple employers, as well as employees who serve as "contractors," are often tempted by opportunities to misappropriate patient-related information for personal financial gain. You can and should attempt to keep track of moonlighting and consulting agreements by requiring your employees to disclose in writing any other employment or contractor relationship they may enjoy at the time of their hire and throughout their employment by you. Also, make an employee's failure to disclose such arrangements an offense that will result in the termination of employment.

### No Expectation of Privacy Policy

You generally have the right to monitor employee use of your computer and communications systems. Employees should be advised that they have no expectation of privacy with regard to the use of company computers, copiers, or data bases, and that you have the right to—and do—monitor all information or data accessed or used by your employees. Fear of electronic detection alone is sufficient to deter many employees from engaging in theft of patient-related information.

### Uniform Trade Secrets Act

Most states have adopted the Uniform Trade Secrets Act (UTSA), which is designed to protect against the

unauthorized disclosure and/or misappropriation of an employer's trade secrets. Under the UTSA, a trade secret may consist of information including a compilation, such as a patient list, that: 1) derives independent economic value from not being generally known to and not being readily ascertainable by proper means by others who can obtain economic value from its disclosure or use; and 2) is the subject of reasonable efforts to maintain its secrecy. Under the UTSA, misappropriation of trade secrets may be remedied by an injunction and /or an award of damages (and, in some cases, an award of punitive damages). In addition, in cases of willful misappropriation, reasonable attorneys' fees may also be assessed against an employee who steals from you. Make your employees aware that if they steal from you, you will seek relief for their misconduct by pursuing your rights against them under the UTSA. As with other employment-related documents, written notice to an employee regarding the UTSA should be maintained in the employee's personnel file.

## **STEP TWO: LIMITING AND MONITORING ACCESS**

It is axiomatic that an employee cannot steal what the employee does not have access to. And, in order to preserve the protections afforded by confidentiality agreements, noncompetition agreements, and the UTSA, access to your confidential and proprietary information must be limited by you and demonstrably subject to reasonable efforts on your part to maintain its secrecy. Accordingly, hard copies of patient lists and related information should be kept in a secure location (preferably under lock and key), and access to these materials should be granted only to those employees who have a legitimate need to review them. Similarly, patient lists and related information that are maintained in a computer should be password protected so that only employees who have need to access these materials can do so. Software that monitors access to your sensitive computer files should be installed and routinely run so that you can see who has accessed these files. Further, in order to prevent electronic distribution of your confidential and proprietary information, you should limit the availability of e-mail and access to the Internet to supervisory personnel, such as managers.

Another increasingly popular cost-saving measure utilized by healthcare providers is to allow employees, such as billers, to work from home and remotely access patient-related information. Keep in mind that an employee (whether working from home or on site) with electronic access to your patient database can download it with nothing more than a memory stick or send it to a personal e-mail database. Software that can monitor employee use and downloading of patient information is now readily available for under \$5000.00. The same software can limit access to patient information, and most importantly

prevent that information from being downloaded or copied. As part of your theft prevention measures, tracking software should be installed to monitor the access, use, and transmission of patient-related information.

## **STEP THREE: PROSECUTING THIEVES AND PURSUING REMEDIES**

Steps one and two will be effective only if your employees firmly believe that in the event of theft, you will seek every remedy available to you. It is perfectly appropriate, as part of your efforts to deter employee theft, to inform your workforce that all instances of suspected employee theft will be promptly reported to law enforcement for investigation and potential prosecution. Fear of conviction and an order of restitution can be a powerful deterrent to employees who are considering stealing from you.

As part of your deterrence efforts, you should also make your employees aware of the civil penalties you may pursue if they steal patient-related information from you, as well as the expenses they will likely incur defending themselves in a lawsuit. Civil penalties can be financially harsh, and the expense of defending a civil suit is something that most employees cannot bear. Perhaps the most potent weapon available to you is a lawsuit seeking temporary and permanent injunctive relief preventing the employee and those who may be acting in concert with that employee from disclosing your confidential information and profiting from its misuse, and damages. Depending upon the circumstances, you may also be able to proceed against the employee for a violation of the UTSA. In addition, as part of your remedy against an employee who has stolen from you, in certain states you may be able to recover, in addition to actual damages stemming from the theft, disgorgement of the monetary value of the employee's compensation (pay and benefits) from the date the employee first began breaching his or her obligations to you through the end of the employment relationship, as well as punitive damages. You may also be able to recover attorneys' fees incurred in connection with litigation relating to employee theft. Many employees who are cognizant of the remedies available to you will likely be dissuaded from stealing from you.

## **CONCLUSION**

Employee theft is not always preventable, but many employees can be dissuaded from stealing from you if you implement the appropriate preventative policies and procedures, limit and monitor employee access to your sensitive files, and vigorously pursue your remedies against employees who turn out to be thieves. The steps necessary to protect your business and keep it profitable are relatively easy to implement and should be undertaken by you as soon as is practicable. ■