



Aspen
Consulting
Group, Ltd.

RISK MANAGEMENT & EMPLOYEE FRAUD

The Association of Certified Fraud Examiners estimated the average loss to a small entrepreneurial organization due to employee fraud at approximately \$127,500.00 per occurrence over an eighteen-month time span. This loss equates to approximately 4.3% of the average revenue of an oncology/hematology practice as reported by the Medical Group Management Association Cost Survey-2002. Employee fraud takes many forms and ranges from the theft of petty cash funds to the embezzlement of hundreds of thousands of dollars. Employees that commit fraud do so in relation to the attributes present in the “Fraud Triangle” (see chart).

Risk from misappropriation of patient and insurance company payments on account constitutes the most common theft by employees in the professional practice. Theft through fraudulent check disbursements from the practice constitutes another high-risk area. Credit card theft has become increasingly more common due to the increased use of credit/debit cards in today’s financial environment.

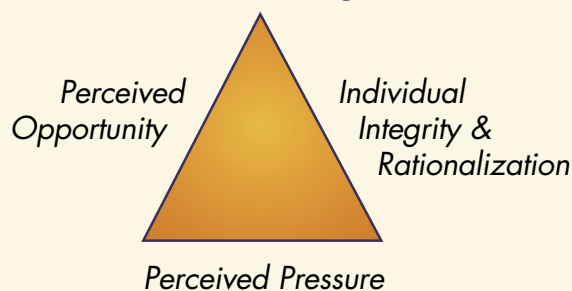
The one ingredient that is always present when employee theft occurs is the *perceived opportunity* identified in the above Fraud Triangle. Therefore, the key to risk management in the professional practice is to attempt the elimination of the *perceived opportunity*. How do you protect your practice from employee theft? The practice must institute and monitor

written practice internal controls and procedures to properly manage the risk from employee theft.

Internal controls may be defined as the procedures and policies established to safeguard the assets of the practice, and to monitor business operational performance effectiveness. Internal controls take many forms and are often referred to as the “checks and balances” instituted to achieve the security of practice assets. The design of appropriate internal controls and procedures is dependent upon the size, experience, and educational level of the staff in relation to the professional organization. Ideally, the concept of “separation of duties” is followed in the design of practice internal controls. For example, the staff individual who records patient and insurance payments on accounts, should not be making the daily bank deposit or reconciling the monthly bank statement. In smaller practices, the separation of duties ideally used with internal controls is not always possible and alternative procedures may need to be instituted to create effective controls.

The organization and written communication of practice internal controls to staff, and the ability to hold staff accountable for their actions is the key to the

Fraud Triangle



establishment of financial risk management policies and procedures. Internal controls should be monitored and periodically tested to ascertain their applicability and effectiveness. Computer passwords and limited access to software applications based on written job descriptions are necessary to reduce the opportunity of employees committing computer fraud. Background checks should be performed on all new employees to assess the presence of prior criminal activity. Finally, the design and monitoring of practice internal controls should be performed by consultants familiar with the healthcare industry and with the daily operational procedures common to the professional practice.

Copyright © Aspen Consulting Group, Ltd. 2003. All Rights Reserved

Direct all correspondence to:
Aspen Consulting Group, Ltd.,
www.aspen-ltd.com; email:
contact-us@aspen-ltd.com.