RM Matters
January 2012

The Dentists Insurance Company
1201 K Street, 17th Floor, Sacramento, CA 95814
800.733.0634 thedentists.com

Electronic Era: Safeguards for Dental Offices

By TDIC Risk Management Staff

Property theft is unfortunately nothing new, however, there are new considerations related to theft in the digital age. TDIC reports about 80 to 100 office theft claims annually with computers, office equipment and digital cameras among the most common items stolen from dental offices. Additionally, TDIC reports an increase in thefts of items taken off site (laptops and patient records) that contain personal health information. The loss of an office computer may seem like a devastating prospect, but a few simple precautions ensure a practice gets back up and running quickly.

Having a backup system for storing information on office computers is critical, according to Sheila Davis, Assistant Vice President of Claims for TDIC. "If dentists have a current backup, they can be back to work either that day or the following day after computer theft," says Davis. "If they don't regularly perform backups, then returning to work can take a week to two weeks, especially if the office is primarily electronic."

Dental offices input an incredible amount of data every week. Testing the backup system does not take long and should be done weekly to ensure it is working and saving uncorrupted and usable data. Store the back up in a secure offsite location so that it does not become part of the theft.

"About 30 percent of theft victims have some sort of issue with backup," says Kyle Broadhead, TDIC claims supervisor. Portable devices such as smart phones have separate limits in the event of data loss, and Broadhead advises against relying on portable devices for storing significant practice-related information.

Keep records of computer and software purchases including receipts and user manuals. These receipts help the claims process move quickly and also ensures replacement computers are compatible with other equipment in the office.

Another consideration in computer theft is the potential for unauthorized parties to access patient information such as Social Security numbers, birth dates and credit card numbers. "Each state has different regulations surrounding the notice requirements for data custodians," according to Davis. "Most states, however, require that the data custodian, in our case the dentist, notify the affected individuals."

Typically, if stolen data contains private information such as a name and date of birth or a name and a Social Security number, the practice owner is required to notify affected individuals informing them of the data theft. Patients can monitor credit reports for any unusual activity. TDIC has a form letter for dentists to use in this situation, and it includes specific recommendations for individuals to secure their credit and prevent identity theft. The Federal Trade Commission offers a free five-step plan online at business.ftc.gov to help business safeguard information.

Using a combination of basic measures will help secure an office. An alarm, surveillance camera and awareness of unmonitored doors and windows go a long way in preventing theft. Broadhead says recent theft claims show a trend in "unforced entry" where an unlocked backdoor or window allows easy entry into an office. Beware of leaving personal items such as purses, wallets or cameras in open areas, and provide a locked cabinet or lockers for staff belongings. When setting up the office, do not place computers near a window.

In the event of any theft always file a police report and in "forced entry" situations, contact police to secure the premises and minimize risk to you and your staff.

TDIC's Risk Management Advice Line can be reached at 800.733.0634.