DENTIST'S ADVANTAGE
PROFESSIONAL LIABILITY & PRACTICE PROTECTION

*The National Society of Dental Practitioners and the Dentist's Advantage Insurance Program for Dentists*

# RISK MANAGEMENT ALERT

## More on HIPAA and Causes of Protected Health Information Breaches

The US Department of Health and Human Services (HHS) reports that a new study suggests that most personal health information (PHI) data breaches in the US from October 2009 through the end of 2017 "haven't been the work of hackers but instead have been due to mistakes or security lapses inside healthcare organizations." The study found that these security lapses can lead to theft of equipment or information, which accounted for 42 percent of PHI data breaches.

The report goes on to say that "another 25 percent of cases involved employee errors like mailing records to the wrong person, sending unencrypted data, taking records home or forwarding data to personal accounts or devices".

To prevent data breaches, it is advisable to transition to digital records and use encryption, firewall protection and cloud-based storage. Never use mobile devices for PHI storage. Additionally, all data containing devices should be located in a very secure area, all employees should receive yearly HIPAA training and employee computer practices be constantly monitored.

HHS takes HIPAA violations very seriously and severe penalties could result from infractions.

A complete review of the HHS report can be found in the November 19, 2018 issue of "Reuters Health" and the November issue of "JAMA Internal Medicine".

For more information on HIPAA topics, such as breach notification, cyber security guidance, and training resources, visit HHS.gov/hipaa.