PROTECT YOUR DATA

Dental office data is a growing target for identity theft and ransomware.

Here's how to protect it!

1. Physically lock up the server and attached backup devices to avoid a data breach as defined by hhs.gov

a. Locate server behind locked door and within a locked, anchored server case

b. Server encryption can also be used to protect data and avoid breach in event of a stolen server

c. Get an alarm system for the office

2. Install a Backup Disaster and Recovery Device (BDR)

a. It's the only known solution to protect against ransomware, the most common tool used by hackers to hijack and ransom a practice's data

b. No need to take hard drives offsite, which substantially limits the chances of data breach

c. The device is encrypted onsite and offsite

d. The device will run your practice when your server can't

3. Have DDS Rescue do a brief one-on-one phone meeting to discuss protecting your valuable server data

What Is Required If Your Office Has a Data Breach?

HIPAA Breach Notification Rule (hhs.gov)

1. Written notification to every patient on record notifying of potential identity theft issues
2. Notify all local media outlets (press release) requirement for 500 or more records
   a. Radio
   b. Newspaper
   c. Television
3. Steps 1 and 2 must be completed within 60 days of discovery of breach

Common Reportable Breaches in Dental Offices

1. Lost or stolen unencrypted notebook computer or external device (backup drive) which contains any patient information
2. Stolen unencrypted server which contains patient data
3. Unauthorized access to the patient data

Search "60 MINUTES IDENTITY THEFT TAX REFUND FRAUD" for more information on how data from dental offices is being stolen and sold.

CONTACT US FOR MORE INFORMATION

800-998-9048 x 102

ddsrescue.com

Pride INSTITUTE "Best of Class" 4 TIME WINNER

DDSRescue™

MONITOR • PROTECT • RECOVER • RESTORE