

Storing and Processing Credit Cards in a Dental Practice

Recently, dental practice management software (PMS) vendors have been contacting dental offices to inform them that due to PCI DSS (Payment Card Industry Data Security Standards), dental offices are no longer able to store credit card information within their PMS. As providers of dental software, these companies are obligated to ensure the software and services they provide to dental offices are compliant with relevant standards.

What is PCI DSS?

The PCI DSS is a set of industry standards designed to protect payment card data. Intended to create an additional level of protection for consumers and reduce the risk of data breaches involving personal cardholder data, the standards are comprised of 12 broad requirements and collectively, more than 200-line item requirements. For example, you must assign a unique account to each person with computer access.

I have a small practice; do I still need to be compliant?

Yes, the PCI requirements apply to all organizations that transmit, process or store data, including those that have a limited number of transactions. Although outsourcing some, or all of your payment processes may simplify them and reduce the scope required for PCI compliance, you cannot ignore it. You need to have policies and procedures in place to protect cardholder data when you get it, as well as when you process charge backs and refunds.

What can happen if my business is not compliant?

PCI DSS compliance is important for many reasons. Failure to comply with PCI requirements can lead to fines and penalties levied by the credit card companies, revocation of credit card payment services or even suspension of accounts. Security oversights can also leave dentists vulnerable to costly and damaging data breaches. Besides making headline news, data breaches can lead to lawsuits, remediation costs, and irreparable damage to a dentist's reputation.

Is PCI DSS a technology requirement?

Yes and no. There are aspects of compliance that deal with technology; however, to be compliant, businesses must adhere to all mandatory standards including technological and non-technological requirements.

Should I store credit card information at my practice?

The general rule is: never store credit card information. There is too much liability if something goes wrong. The only business reason for storing credit card numbers is recurring payments. However, you have several responsibilities if you support recurring payments. You must follow the terms of your merchant agreement.

What date does this take effect?

PCI DSS compliance is already in effect. You should be taking steps now to ensure your practice is compliant.

Where can I get more information?

You can find more detailed information at www.pcicomplianceguide.org