SEO DETAILS:

Page Title: PCI Data Security Standards for Health Care Practices | [INSERT RELATED SERVICE] | [INSERT FIRM NAME]

Meta Description: [NAME OF FIRM] explains why compliance with PCI standards can help health care practices avoid data breaches.

Headline: Health Care Industry Should Bolster Credit Card Data Protections

BODY COPY:

As credit card payments become more and more ubiquitous for health care consumers, health care practices should continuously monitor their handling of financial transaction information and ensure compliance with Payment Card Industry (PCI) data security standards.

PCI standards apply to any business involved in credit card transactions, requiring them to provide a secure environment for the storage and transmission of data. Long applied to retailers, PCI compliance is a growing issue for hospitals and practices to consider. Many patients have co-pays, and with the increase in high-deductible plans, they have to foot the majority of the bill for a longer period of time.

Data breaches are also becoming more common for health care businesses. According to an annual report by Trustwave Global Security, which measures data compromises by industry, health care companies saw a notable uptick in incidents between 2016 and 2017.

PCI standards can help companies prevent the exposure of sensitive data. Data breaches themselves carry substantial financial costs, but health care practices must also follow these standards carefully to ensure successful audits. PCI data security violations can result in heavy fines imposed by payments processors.

The protocol to follow depends on the manner in which a business is involved in credit transactions. Requirements would differ for a health care practice depending on the type of payment terminal the practice uses and how it stores or transmits the payment data.

The PCI Security Standards Council sets the applicable data security guidelines and maintains an FAQ that explains the compliance process. Among other things, health care companies need to:

- **Build and maintain a secure environment for the handling of credit transactions.** Simple, but important, compliance standards include changing default passwords for off-the-shelf products and using strong passwords for login access.

- **Carefully secure cardholder data during storage and transmission.** Even if a healthcare practice doesn't store sensitive payment data itself, only use trusted third-party vendors for transactions. If payment data will go over any public or open network in the transmission process, make sure that the data is properly encrypted.

- **Manage and restrict access to sensitive payment information.** Limit access to credit payment data to those who need it and monitor who accesses that data and when.

- **Conduct regular tests of security systems and protocols.** Verify that network access and cardholder data access looks correct. Test whether systems are still being used properly and check for possible vulnerabilities in software or processes.

- **Maintain information security policies for people to follow.** Document all of these procedures and protocols so that all employees understand their responsibilities in following PCI data security standards.

PCI compliance violations can lead to fines of thousands of dollars or more. The liability from a data breach can exceed those costs substantially. As health care practices handle more credit transactions and become bigger targets of cyberattacks, they should be prepared to demonstrate PCI compliance.

CLOSE:

Please contact [NAME] in our [DEPARTMENT] at [NUMBER/EMAIL].

SUGGESTED IMAGERY:

https://stock.adobe.com/images/credit-card-payment-security/212182285?prev_url=detail