How Secure is Your Patient Credit Card Data?: 5 Actions to Take Now
By Cheryl Toth, MBA, KarenZupko and Associates, Inc.

Recently, I learned that a cosmetic practice client guarantees new patient consultations by taking patient credit card numbers over the phone, and entering them into the computer system's free-form "notes" field. "We never run the patient's credit card until they come in for their appointment," explained the Patient Coordinator. "After we run it, we delete the number."

This Patient Coordinator is top-notch and the practice is very successful. But what she and staff are doing with credit card numbers is not only risky, it's prohibited under the Payment Card Industry (PCI) Security Standards, developed by Visa®, MasterCard®, Discover® and American Express®, to reduce the risk of credit card fraud and identity theft. That's because "notes" fields are not secure, not encrypted, and everyone in the practice has access to the data.

"It's all too common for practice staff to take a credit card number over the phone, write it on a sticky note or patient chart, or put it in the computer system in a place where they assume it's safe," says Kathleen Ervin, Vice President, Relationship Management at TransFirst. "But these are big no-no's."

According to PCI Compliance standards, all credit card data must be entered and stored in secure and encrypted systems, with no more than the last four digits of the card number visible. This is easily accomplished with today's credit card or Web-based terminal. Following PCI compliance standards reduces the risk of data theft and identity fraud – which is why Visa and MasterCard require that both processors and their merchants be compliant.

For dermatology practices, big hacking schemes – such as the one famously endured by the retail giant Target last fall – are not the biggest data threat. ***Your employees and billing service staff are***. In fact, a healthcare attorney colleague has worked on five billing company or practice embezzlement cases in recent memory, and says data theft in medical offices is fairly easy because staff and billing services are given easy access to a wide range of patient identity data.

Securing this data is serious business. According to Ervin, if your credit card data is breached, Visa and MasterCard could fine your practice, and based on the severity of the breach, limit your ability to accept credit cards again. More importantly, Ervin notes, "you can lose your patients' trust," which could lead to patients leaving the practice and significant revenue loss. "This is the new reality of taking credit card payments."

If your practice is writing credit card numbers in the patient's chart, sending them in an unsecured email to the billing service, or including them on a spreadsheet along with a patient's agreed-upon monthly budget plan amount, it's time to make some changes. "PCI compliance is all about protecting a patient's credit card data," Ervin says. "You would not leave protected health information (PHI) lying on your desk or in an insecure location. You've got to think the same way about credit card data too."

Take these five actions to ensure this data is safe:

1. **Review current processes.** "In light of the recent Big Box breaches, it's more important than ever to understand what staff are doing with patient credit card data," Ervin says. If they are keeping it in Excel spreadsheets (printed or digital), computer system comment fields, or pieces of paper that aren't immediately shredded, all of these practices must be discontinued. And don't assume a phone

message that's shredded has you off the hook. Ervin knows of one practice that included credit card numbers in its phone message book, forgetting it had carbon copies.

2. **Destroy data on paper.** "If staff take a credit card number over the phone and write it down before entering it into a credit card machine, they must shred it immediately afterward," insists Ervin. "They can't leave it on their desk, or go to lunch, or get a cup of coffee. You never know who may walk by – a maintenance worker, cleaning staff, a patient. There are very smart people out there who are looking for personal identity data that they can steal and either use or sell," Ervin says.

   In a perfect world, staff would never ask for a credit card number over the phone or write it on paper. "The most secure way to accept credit cards is to direct patients to enter their payments online in a secure system, or swipe their credit card in the office using a Web-based payment system or credit card terminal," explains Ervin. These tools ensure the data is encrypted and stored securely, and that *no one* in your practice has access to full numbers.
3. **Switch to Web-based payment processing.** TransFirst, PayPal and A-Claim all offer web-based processing services. Such services allow staff to take payments or establish recurring payment plans right from their computer.
4. **Get PCI certified annually.** Your credit card processer will walk you through the security and risk assessment and provide a certificate. "If your data is breached, you can be fined for every incident," reminds Ervin. Make it a standard practice to get recertified each year.
5. **Purchase breach coverage**. Even if you are compliant, you might still suffer a breach. Breach coverage helps cover notification costs, legal fees, and other expenses.

Says Ervin, "PCI compliance is a fairly new standard, and it's not to be taken lightly. You already understand the importance of HIPAA. Take the same approach with staff about taking and storing credit card data. A little bit of vigilance goes a long way."

Cheryl Toth, MBA is a Practice Leadership & Implementation Coach with KarenZupko & Associates. She is passionate about leveraging technology to work smarter and coaching practice leaders to thrive in the midst of chaos, information overload, and change. Cheryl brings 20 years of consulting, training, technology product management, and marketing to her projects.

Originally in September/October 2014
Tag: Other